

**GUIDO GLUSCHKE
PROF. DR. MESUT HAKKI CAŞIN
MARCO MACORI (EDS.)**



CYBER SECURITY POLICIES AND CRITICAL INFRASTRUCTURE PROTECTION

CYBER SECURITY POLICIES AND CRITICAL INFRASTRUCTURE PROTECTION

***Guido GLUSCHKE, Prof. Dr. Mesut Hakkı CAŞIN,
Marco MACORI (Eds.)***

Copyright © 2018 by Institute for Security and Safety (ISS) Press

All rights reserved.

No part of the material protected by this copyright notice may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any informational storage system without written permission from the copyright owner.

ISBN 978-3-00-058988-1 (print)

ISBN 978-3-00-060505-5 (pdf)

Institute for Security and Safety GmbH

David-Gilly-Str. 1

14469 Potsdam

Germany

Phone: +49 331 58148330

Email: info@uniss.org

Web: www.uniss.org

TABLE OF CONTENTS

FOREWORD	vi
CONTRIBUTORS	vii
Strengthening the Legal Framework for the Physical Security of Nuclear Materials for the Future of Nuclear Renaissance: Risks, Opportunities, and the Case of Turkey <i>Mesut Hakkı Caşın</i>	1
Critical Infrastructure Security Paradigm and Modern Protection Policies <i>Robert Radvanovsky</i>	57
Securing Our Critical Infrastructures <i>Jane Leclair, Scott Burns</i>	69
Cyber Security Policies for Critical Energy Infrastructures in Korea Focusing on Cyber Security for Nuclear Power Plants <i>Oh Il Seok (Luke), Kim So Jeong</i>	77
The Future of Nuclear Energy Security <i>Mesut Hakkı Caşın</i>	97
Cyber Security of Nuclear Power Plants <i>Guido Gluschke</i>	123
Cyber Security for Nuclear Installations <i>A. Beril Tuğrul</i>	139
CIP Security Awareness and Training: Standards and Practice <i>Rafał Leszczyna</i>	149

Cyber Security Education and Training for Critical Infrastructure Protection	167
<i>William Hurst, Nathan Shone, Carl Chalmers</i>	
The Importance of Public-Private Partnerships in Critical Infrastructure Protection	183
<i>David Sutton</i>	
Public and Private Sector Energy Infrastructure and Cyber Information Sharing	199
<i>Ernest N. Hayden</i>	
The Threat of Cyber Terrorism – A Risk Management Perspective	225
<i>Marco Macori</i>	
Nuclear Energy and Cyber Security Domain at Crossroads in Digital Technologies New Phases	237
<i>Mesut Hakkı Caşın</i>	
Charting Critical Energy Infrastructures Dependencies on Space Systems New Frontiers in Risks, Vulnerabilities and Threats	273
<i>Liviu Mureşan, Alexandru Georgescu, Ştefan Popa, Ştefan-Ciprian Arseni, Iulia Jivănescu</i>	
Threat Intelligence for CIP	295
<i>Oscar Serrano</i>	
Understanding NATO's New CIP Policies: Common Efforts and Solidarity	311
<i>Mesut Hakkı Caşın</i>	
Implementing Cyber Security According to National Regulations and International Standards	321
<i>Kristina Sander, Guido Gluschke</i>	
Balancing Cyber and Physical Defense in the Energy Sector: Nuclear Energy Lessons Learned	331
<i>Dmytro Cherkashyn</i>	

**A Pragmatic and Structured Method to Secure the Systems
That Control the Nuclear Environment**
Özkan Demiröz

341

ABBREVIATIONS

371

FOREWORD

As energy infrastructures have become a lifeline for modern economies and developed societies, these infrastructures have to be considered as highly critical. Various different views on protecting such energy infrastructures against certain threats are covered in the chapters of this book. While most works focus on technical aspects and other books focus on policy aspects, this book tries to convince by a balanced mix of perspectives on threats, organizational approaches, and protective measures. It is worthwhile to mention that the book covers some chapters on nuclear security, which is an added value for newcomer states, such as Turkey, which made the decision that this kind of energy suits its energy needs.

With around one third of the chapters focusing on cyber security, this book reflects the latest threat landscape in the energy sector and addresses an audience that is interested in learning more about global emerging threats. Cyber is an underestimated part of critical infrastructure and has become an essential part of national security today. By now, not every nation state is aware of this situation and the possible consequences for its economy. Thus, the book raises awareness by comprising topics such as capacity building, standards and cyber security policies. With that the authors give insights that might help states develop their own security strategy in terms of the cyber-energy complex.

The book also comprises NATO's view on critical infrastructure protection, which helps the reader understand this issue from a military perspective, and furthermore from a perspective of transnational organizations that are facing distinctive challenges. Even if not all kinds of energy are touched, in particular renewables, the book has high relevance, gives a comprehensive view on multiple dimensions of energy security and can be easily understood by readers who do not have a background in energy security. On the one hand it is very helpful for readers who expect to get insights from experts in this field, on the other hand it can be of use for educational purposes and capacity building.

Guido Gluschke
Co-Director
Institute for Security and Safety (ISS)
at the Brandenburg University of Applied Sciences

Potsdam/Germany
September 2018

CONTRIBUTORS

Ştefan-Ciprian Arseni is a Lieutenant Engineer and a Scientific Researcher at Military Equipment and Technologies Research Agency, Romania. He is currently a PhD candidate at the University “Politehnica” of Bucharest. His research interests include computer, network and space security, network management, software engineering.

Scott Burns is a Digital Systems and Cyber Security Project Manager with First Energy Nuclear Operation Company at the Perry Nuclear Generating Station in Perry, Ohio. He is Responsible for the implementation of the Perry Cyber Security Program as required by 10CFR73.54 Protection of digital computer and communication systems and networks. His duties also include responsibilities for all aspects of program development, including implementing procedures, development and delivery of training modules, and cyber security field assessments.

Mesut Hakkı Caşın is a Professor and Head of the International Relations Department at İstinye University in İstanbul, Turkey. He is an expert on international law, terrorism, international security strategies, energy politics, and military history. He gives lectures on international relations and international law at the graduate and undergraduate levels.

Carl Chalmers is a PhD student in the Department of Computer Science at Liverpool John Moores University. He received a BSc (Hons) with distinction in Computer Science from LJMU in 2014. His current research interests include critical infrastructure, smart technologies, health monitoring, data classification, and data mining.

Dmytro Cherkashyn holds a M.Sc. degree in nuclear energy from the Sevastopol National University of Nuclear Energy and Industry, in Ukraine. Prior to his current position as nuclear security scientist at the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, he was a senior teacher at the nuclear energy facilities department. His areas of research also include nonproliferation, international cooperation on nuclear safety and security, and cyber security for nuclear facilities.

Özkan Demiröz is the founder of Demiroz Consultancy B.V., a cyber security consultancy firm located in the Netherlands. He holds an academic Master degree in Information Security (MSIT) from the Eindhoven University of Technology and is a senior cyber security consultant with many years of experience in information security, cyber resilience, risk management, and privacy within governmental, critical and vital organizations. Some of his most prominent work was in regard to a large Dutch,

German, British, US and French nuclear project for which he was the cyber security subject matter expert interfacing with the regulatory agencies.

Alexandru Georgescu is a Research Fellow with the EURISC Foundation. He has studied Economics, then Geopolitics, and now pursuing a PhD in Risk Engineering for Critical Infrastructure Systems. He is emerging as a notable member of the new generation of Romanian security experts. His main study fields include geopolitics, international security issues and critical infrastructure protection.

Guido Gluschke is one of the directors of the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences. He is an expert in cyber security in the nuclear context. His main areas of expertise are IT and cyber security, especially in the energy context. He is part of nuclear-cyber projects of the Nuclear Threat Initiative, Washington, and a member of the Energy Expert Cyber Security Platform - Expert Group of the European Commission Directorate General of Energy, Brussels.

Ernest Hayden is an Executive Consultant at Securicon, LLC, has held roles as Global Managing Principal – Critical Infrastructure/Industrial Controls Security at Verizon. His primary emphasis is on project and business development involving cyber and physical security of industrial controls, smart grid, energy supply, and oil/gas/electric systems and facilities with special expertise on industrial controls. He is a frequent author of blogs, opinion pieces and white papers.

William Hurst is a Senior Lecturer in the Department of Computer Science at Liverpool John Moores University (LJMU). He holds a PhD in critical infrastructure security. His research interests include critical infrastructure protection, cyber security, data classification, simulation and 3D graphics.

Kim So Jeong is a senior researcher and leads the Cyber Security Policy Division of National Security Research Institute in Korea. She received her PhD in Engineering from the Graduate School of Information Security, Korea University.

Iulia Jivănescu is currently a graduate student at the Massachusetts Institute of Technology in the field of Astronautics and a research scientist with the Romanian Space Agency.

Jane LeClair received her doctorate from Syracuse University and served as Dean of the School of Business and Technology at Excelsior College in Albany, NY prior to assuming her current position at NCI. She is an ongoing consultant with the International Atomic Energy Agency (IAEA). She has written and edited numerous books, journals and articles related to cyber security and technology. Her latest book, "Cyber Security in Our Digital Lives" was just released.

Rafal Leszczyna is an Assistant Professor at Gdansk University of Technology, Faculty of Management and Economics. He holds the MSc degrees of Computer Science and Business Management. He has a PhD in Computer Science, specialization – Computer Security at the Faculty of Electronics, Telecommunications and Informatics of Gdansk University of Technology. His professional interests include the security of information systems, information security of critical infrastructures, and the issues relevant to information security management.

Marco Macori is a Research Fellow with the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences in Germany. His research focuses on the nexus of transnational terrorism and cyber threats, an issue on which he lectured at the NATO Center of Excellence - Defence against Terrorism, *inter alia*. He holds degrees in Political Science and English from the University of Trier. He's a member of the academic steering group for the OSCE research project on Cyber CBMs, and of the Transatlantic Cyber Forum of Stiftung Neue Verantwortung.

Liviu Mureşan is a noted Romanian security expert, with significant international experience. He currently leads the EURISC Foundation, a private research institute, and has been a promoter of critical infrastructure protection activities since the field's inception, contributing also to Romania's development of a competitive framework for such activities.

Ştefan Popa is a Captain Engineer, Scientific Researcher and Head of the Communications Systems Laboratory at Military Equipment and Technologies Research Agency, Romania. He received his Master's Degree in Computer Science from the Military Technical Academy in Bucharest. His research interests include network security and management, space systems protection.

Robert Radvanovsky is the owner of the SCADASEC mailing list for SCADA and control systems security discussions, while working as an active participant with several U.S. Department of Homeland Security cyber security working groups. He is an active professional in the United States with knowledge in security, risk management, business continuity, disaster recovery planning, and remediation.

Kristina Sander holds a M.Sc. degree in the field of technology from the Karlsruhe Institute of Technology (KIT), Germany. Her main areas of expertise are IT/cyber security and information protection in the energy context. She works for the international security management consultancy VICCON and is a Research Fellow with the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences.

Oh Il Seok (Luke) is the President of Korean Legislation and Policy Research Institute, a senior paralegal at Wonjin (Law Firm), lecturer at Korea University, and senior

research fellow at Korea University Legal Institute. He holds a PhD in Law from Korea University and an LLM from Northwestern University School of Law.

Oscar Serrano currently works for the NATO Communications and Information Agency as Senior Scientist in cyber defense, working mainly in Cyber Security policy and Risk Management. His research interests include Risk Management, Threat Information Management and Detection of Advanced Persistent Threats.

Nathan Shone is a researcher currently working as part of the PROTECT research center in the Department of Computer Science at Liverpool John Moores University (LJMU). He also holds a PhD in network security, studying misbehavior detection in complex system-of-systems, which was awarded by LJMU in 2014. His research interests include complex system security, security monitoring, IoT security and digital forensics.

David Sutton was a tutor on the distance learning course for the Master's degree in Information Security at the Royal Holloway University of London, is co-author of 'Information Security Management Principles', and author of 'Information Risk Management: A Practitioner's Guide', both published by BCS, The Chartered Institute for IT. Since retiring from O2, he has undertaken a number of CIIP-related projects for the European Network and Information Security Agency (ENISA).

A. Beril Tuğrul has been a Professor at the ITU Energy Institute. She was the Head of Nuclear Researches Division between 2008 and 2015 and has been lecturing in Gebze Technical University and also Military Academia on energy policy. She was Vice President of the Turkish Atomic Energy Authority Nuclear Safety Committee from 1998 to 2000. She was also member of the Turkish Atomic Energy Authority Consulting Committee between 1997 and 2003. She has over 300 publications. She gained many publication awards from ITU, Turkish Scientific and Technology Council, and Turkish Scientific Academy.

STRENGTHENING THE LEGAL FRAMEWORK FOR THE PHYSICAL SECURITY OF NUCLEAR MATERIALS FOR THE FUTURE OF NUCLEAR RENAISSANCE: RISKS, OPPORTUNITIES, AND THE CASE OF TURKEY

Prof. Dr. Mesut Hakkı CAŞIN

ABSTRACT

Although the Cold War came to an end without an open warfare between the members of the NATO and the Warsaw Pact, the nuclear security issues continue to be on the front cover of the global agenda. There are 3 basic elements identifying the paradigm transformation on nuclear security: The first is North Korea's nuclear proliferation crisis raising concerns at the Pacific region. US Secretary of State Tillerson explained that military option remains on the table. Pentagon has deployed an aircraft carrier to the Korean Peninsula that includes missile defense systems. The second is that, in spite of states' legally binding promises to keep nuclear materials secure, illicit nuclear smuggling and nuclear terrorism threats rose to worldwide transboundary structures. Major unlawful criminal acts and breach of nuclear physical security will most likely occur in the form of suicide attacks, sabotages, and cyber-attacks on nuclear plants, which will bear highly serious safety risks, endangering public health. Third, of course, is the usage of nuclear energy for peaceful purposes which are the reality of many modern and developed societies. Indeed, these states are building 60 new reactor plants under the so called "Nuclear Renaissance" to develop nuclear energy on global level. Initially, international common security mechanisms have served as critical steps in contribution to improve nuclear security, particularly to reduce the risk of the thievery of nuclear and radioactive materials, technology and expertise from the USSR. International law also regulated the states' responsibility measures which improved in the past four decades. Finally, it could be argued that to have effective, sustainable solution against new nuclear physical threats, we need to achieve worldwide cooperation, build confidence dialogues that would have all states working together on risk management; raising the awareness of decision makers on their international law responsibilities. Thus, this paper's aim is to academically search the ways of globally improving the security of nuclear materials globally and to discuss a road map for Turkey by comparing the best practices of nuclear material protection worldwide while benefitting from IAEA's extensive capabilities.

Key Words: Legal Framework, Physical Security Of Nuclear Materials, Nuclear Renaissance

1. Why Is The Nature of Global Nuclear Threat Changing From The Struggle Between and Warsaw Pact to The North Korean Nuclear Challenge?

In this article, our basic idea is to examine the effects of the braking/ balancing mechanism, which prevented a possible nuclear war between members of the NATO and the Warsaw Pact in the theoretical plane, and of the bipolar forces of equilibrium that resulted in potentially effective results. In other words, the two defense circles did not go to the point of using nuclear force as a solution to their conflicts as they withheld the deterrence factor in the foreground, despite the presence of thousands of nuclear weapons in their stocks. After the disintegration of the Warsaw Pact and the dissolution of the USSR, NATO renewed its nuclear policy. Taking the 2008 Georgia and 2014 Ukraine Crisis into account, NATO has finally resolved the concept of nuclear deterrence, in spite of the reduction of nuclear weapons, in accordance with Article 5 of the Washington Treaty, under the "Securing the Indivisibility" principle.

There is a fundamental change in the use of nuclear energy for peaceful purposes and for the use of nuclear weapons in international relations. As it is well known, the first nuclear weapons were used during the WWII in Hiroshima and Nagasaki. The destructive capability of these weapons have not significantly increased in the past 70 years, yet the time it takes to hit targets between airplanes, planes and submarines and continents fell below the quarter-hour mark. During the Cold War, the nuclear arms race between NATO and the Warsaw Pact gave way to crises in Cuba, Berlin, Czechoslovakia and Hungary, and drew rising parabolas. The weapon agreements of INF and START, along with detente policies between the USA and the USSR, have increased military and political pressures on the front of nuclear proliferation. At this point, the international narratives attempting to avoid the dispersion of nuclear weapons have been effective in the last period of the Cold War. Nevertheless, despite the disintegration of the USSR and the Warsaw Pact, NATO and the EU are extending towards the East, and thus the policies on the acquisition of nuclear weapons of actors such as North Korea have dragged the post-Cold War global security parameters into an unbalanced position.

Understanding this critical phenomenon requires an analysis of the relationship between the utilization of peaceful nuclear energy, and the possession of nuclear weapons, or of the options of attacking nuclear facilities by illegal states or non-state actors as an instrument for their terrorist movements and intentions.

- Why should the international community seek to limit the proliferation of nuclear weapons, and attempt to prevent the escalation of and ease the nuclear conflict with the North Korean challenge?
- If there is not a peaceful solution in the case of North Korea, can it develop into a regional nuclear conflict?

- Can the detente policy between the NATO and Warsaw Pact be a model for the Pacific, and form a theoretical basis as well? Will NATO play its part in the resolution of future disputes, and change its nuclear strategy?

Nuclear weapons today not only present tremendous danger, but also provide an historic opportunity. Nuclear weapons were essential to maintain international security during the Cold War, because they were a means of deterrence.¹ There are two broad theoretical views on the question of the causes of nuclear proliferation. The first opinion takes the “realist” view that states acquire nuclear weapons because their security demands it. In other words, states, in international anarchy, need to deter potential attackers; and in the nuclear age, the gold standard of deterrence is nuclear. The second opinion holds the “idealist” view that states obtain nuclear weapons because they learn to “stop worrying and love the bomb” (to coin a phrase). In other words, states are driven toward nuclear armament by the thought that their possession is beneficial or necessary, but this idea is not a simple function of the exigencies of international anarchy, as is indicated by its very uneven acceptance around the world.²

In terms of the international balance of power theory, at the heart of Cold War had been a high intensity arms race encompassing the nuclear and conventional dynamic military between NATO and Warsaw Pact. Military balance between two poles evolved to place importance on the possibility of utilization of stockpiled nuclear forces during military confrontation with the European nations’ main involvement being partaking in the deliberations on the subject. To compensate for the conventional superiority of the Soviet Union and Warsaw Pact, nuclear weapons have clearly dominated the development of NATO strategy since 1949, Therefore, each blocks’ framework have been founded within the bipolar balances’ nuclear order, guaranteed to supply nuclear umbrellas extended over allies of the US and the USSR.³

In this regard, at the first quarter of the 21st century, international system and nuclear security policies has already brought a number of unwelcome surprises, including triggering the 11 September terrorist attacks and the international network surge of radical terrorism and nuclear proliferation threat, also challenges rising from regimes not heeding the rule of law and the norms of international law, such as North Korea. Indeed, the attacks of September 11 2001 demonstrated the potential destructiveness of even a small group of extremists. However, what I am arguing here is that this event, with the apparent goal of inflicting mass casualties among the civilian populace, underscores the importance of keeping weapons of mass destruction out of the hands

1 George P. Shultz, William J. Perry, Henry A. Kissinger and Sam Nunn: “A World Free of Nuclear Weapons”, *The Wall Street Journal*, January 4, 2007; Page A15.

2 Jacques E. C. Hymans: “Theories of Nuclear Proliferation”, *The Nonproliferation Review*, 2010, Vol. 13, No. 3, pp. 455-465.

3 Mesut Hakkı Caşın: “Uluslararası Güvenlik Stratejileri ve Silahsızlanma”, Milli Savunma Bakanlığı, Ankara, 1994, s. 88-167.

of such groups. The ongoing struggle to protect innocent people from violent extremists will likely continue for years to come.⁴

In contrary to NATO's collective defense idea, Warsaw Pact's operational plans were based on the concept that under a possible NATO attack, they would resist and very soon begin a counter-attack involving the invasion of the aggressors' territory resulting in its occupation.⁵ In this framework, nuclear and chemical weapons would have been used in the assault on NATO forces in West Germany, even if NATO solely used conventional weapons.⁶ NATO transformed its missions, expanded its membership and perched its military footprint and political commitments far from the inter-German border that was the pivotal point of Cold War security dilemmas.⁷ On the positive side, the end of the Cold War era greatly reduced the threat of an all-out nuclear war between the US and the Russian Federation; however it created a new set of challenging international security concerns and revisionist movements either by states or non-state actors. Thus in formation of the new world order, despite greatly reducing the number of nuclear weapons and dissolution of the Warsaw Pact, NATO allies effectively decided that nuclear weapons must be kept in terms of making deterrence more credible by demonstrating 'alliance solidarity' factor by then "in a small box somewhere in the corner and that is where they should stay".⁸

Following the examination of nuclear balance between NATO and Warsaw Pact, it is assumed that the understanding of North Korean Crisis' different characteristics do form an important example for nuclear non-proliferation and world peace. As a matter of fact, North Korea causes the tension to increase in the Pacific region, entering into a challenge to accept nuclear power as a different actor apart from the inter-block power balance. From this point of view, the understanding of diplomatic, military and legal endeavors for the prevention of regional countries and the proliferation of nuclear weapons is considered to be an example of the solution of future disputes. North Korea has withdrawn from the NPT Treaty in its first step, with its gradual nuclear work. North Korea has subsequently accelerated the increase in the range of nuclear weapons it has acquired with its new ballistic missile tests, while also banning its nuclear tests to the international public. North Korea, by de facto acquiring the status of nuclear nation in this way, not only constitutes a new step forward in the danger of nuclear proliferation, but has also triggered a different crisis by threatening South Korea, Japan, US and the regional alliance against this development. In this respect, it is the

4 Thomas K. Scheber: "U.S. Nuclear Policy and Strategy and the NPT Regime-Implications for the NATO Alliance", *Comparative Strategy*, Vol. 26, No: 2, 2007, pp. 117-126.

5 Christoph Bluth: "Offensive Defence in the Warsaw Pact: Reinterpreting Military Doctrine", *Journal of Strategic Studies*, Vol.18, Issue 4, 1995, pp.55-77.

6 Lothar Ruhl: "Offensive Defence in the Warsaw Pact", *Survival*, Vol.33, Issue 5, 1991, pp.442-450.

7 Stephen J. Cimbala & Peter Kent Forster: "The US NATO and military burden sharing: post-Cold War accomplishments and future prospects", *Defense & Security Analysis*, Vol. 33, No. 2, 2017, pp. 115–130.

8 Martin A. Smith: "In a Box in the Corner"-NATO's Theatre Nuclear Weapons, 1989–99", *Journal of Strategic Studies*, Vol.25, No.1, 2002, pp.1–20.

main idea of this article is discussing today's difference with the nuclear deterrence mechanism between the East and West Blocks in the bipolar forces balance in the Cold War era, and preventing future nuclear crises and the nuclear confrontation. The example of North Korea would serve as a possibility to understand the main differences between nuclear sprawl and the state of war in the context of realistic politics, and the corresponding escalation of the threat of nuclear terrorism by non-state actors.

Democratic People's Republic of Korea or North Korea (NK) has announced its decision to withdraw from the NPT on January 10, 2003. After this development, Pyongyang's first nuclear test occurred in 2006. The North claimed to have launched ballistic missile from a submarine on 24 August, which landed in Japanese waters, which was another indication of progress in its missile development. NK has declared conducting its fifth and strongest nuclear test at its Punggye-ri site nuclear test on September 9, 2016.⁹ Against this show of power, the US-South Korea-Japan troika have strongly opposed and protested the Pyongyang regime. White House's reaction was put forward by President Obama, highlighting that 'the United States does not and never will, accept North Korea as a nuclear state'.¹⁰ Also, former Secretary of State, John Kerry said that the test is 'a grave threat to ... international peace and security ... as destabilizing as it is unlawful'.¹¹ Seoul administration also urged North Korea, 'to immediately abandon its nuclear weapons and missile programs'. The Japanese Prime Minister Shinzo Abe evaluated the NK's nuclear test as being 'totally unacceptable'.¹² US president Trump said that his earlier "fire and fury" comments were towards North Korea. He also said that "military solutions are now fully in place, 'locked and loaded,' should North Korea act unwisely".¹³ It's pretty clear that if North Korea actually launches a nuclear-tipped missile that explodes and causes large-scale casualties in Japan, South Korea, the United States, or anywhere else, nuclear retaliation against North Korea is likely. What's more difficult is to predict are

9 "North Korea's Fifth Nuclear Test", *Strategic Comments*, Vol.22, No. 8, 2016.

10 Kelly McLaughlin: "Obama Slams North Korea's Nuclear Weapon Pursuit and Warns Kim 'Must Face Consequences' as He Speaks in Seoul After Wrapping up His Ten-day Family Vacation in Indonesia", *Daily Mail Online*, 3 July 2017,
<http://www.dailymail.co.uk/news/article-4660572/Barack-Obama-slams-North-Korea-s-nuclear-weapon-pursuit.html>.

11 Charlie Bayliss: "Nuclear Backlash: US to Unleash 'Overwhelming Response' to North Korea if it Launches Nuke", *The Daily and Sun Express*, 20 October 2016,
<http://www.express.co.uk/news/world/723204/North-Korea-US-Ash-Carter-John-Kerry-nuclear-weapons-south-korea-kim-jong-un>.

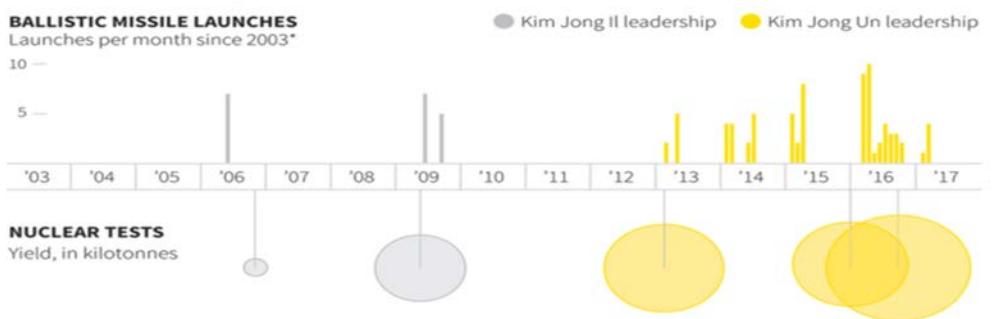
12 Tom Phillips: "Trump Vows 'All Necessary measures' to protect allies from North Korea, says Abe", *The Guardian*, 31 July 2017,
<https://www.theguardian.com/world/2017/jul/31/trump-vows-all-necessary-measures-to-protect-allies-from-n-korea-says-abe>.

13 Jesse Johnson: "Trump to speak with Abe and Xi as North Korea nuclear issue looms large", *The Japan Times*, 2 July 2017,
<https://www.japantimes.co.jp/news/2017/07/02/national/politics-diplomacy/trump-speak-abe-xi-north-korea-nuclear-issue-looms-large/#.WZ6QQT5JbIU>.

the outcomes of a number of action scenarios that are still provocative and escalatory.¹⁴

North Korea missile launches

North Korea fired four ballistic missiles early on Monday, three of which landed in Japan's exclusive economic zone, Japanese Prime Minister Shinzo Abe said. The frequency of the country's missile and nuclear tests has increased under Kim Jong-Un.



*Data compiled by Center for Strategic and International Studies (CSIS) since 2003. Shows ballistic missiles only and does not include surface-to-air, surface-to-ship missiles or rockets. Data as of March 6, 2017.

Source: Center for Strategic and International Studies (CSIS); Reuters

Reuters

Source:

https://gdb.voanews.com/09E55497-F225-465E-9F38-6F4C6870DB24_w650_r0_s.png

As Tokyo warned citizens in the north of the country to take cover, North Korea's fourth missile test in four days at last fired a missile over Japan. It was North Korea's 13th launch of ballistic missiles in 2017.¹⁵ Tokyo and Washington have requested an urgent meeting of the United Nations Security Council after Pyongyang launched a missile over the Japanese island of Hokkaido.¹⁶ President Donald Trump said "all options are on the table" in terms of a US response to North Korea's launch of a missile over Japan. Trump said that North Korea has "signaled its contempt for its neighbors, for all members of the United Nations, and for minimum standards of acceptable international behavior" with the missile launch. He also added, "Threatening and destabilizing

14 Herbert Lin: "War Clouds on the Korean Peninsula: What Would We do If...?", *Bulletin of the Atomic Scientists*, 11 August 2017, <http://thebulletin.org/war-clouds-korean-peninsula-what-would-we-do-if%E2%80%A611016>.

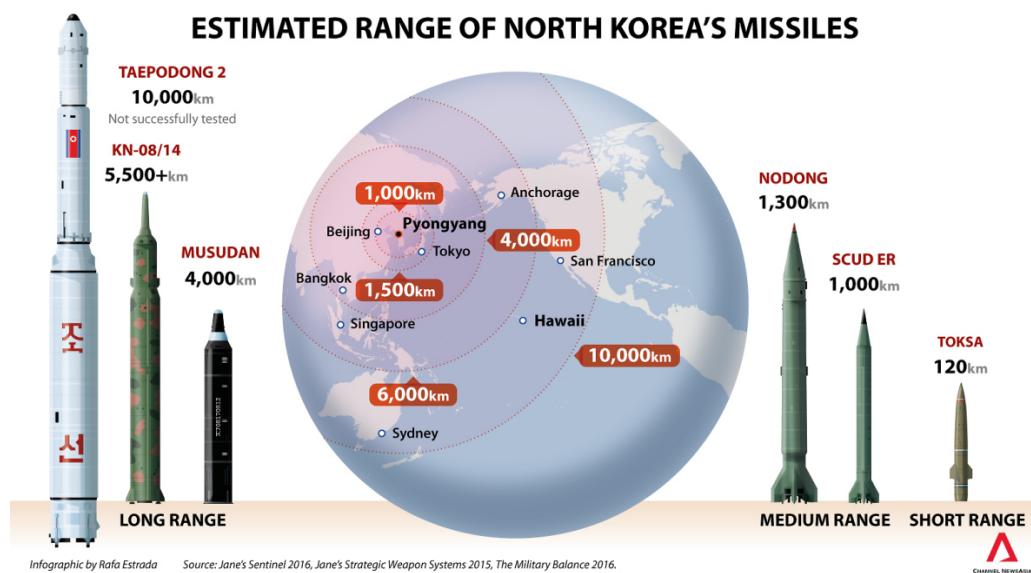
15 Seoul's Joint Chiefs of Staff said the missile traveled around 2,700 kilometers (1,677 miles) and reached a maximum height of 550 kilometers (341 miles) as it flew over the northern Japanese island of Hokkaido. The launch, which appears to be the first to cross over Japan since 2009, will rattle a region worried that each new missile test puts the North a step closer toward its goal of an arsenal of nuclear missiles that can reliably target the United States. It appeared to be the North's longest-ever missile test, but South Korean officials couldn't immediately confirm. "Japan, US Seek to Up Pressure after North Korea Missile Launch", *Times of Israel*, 29 August 2017, <http://www.timesofisrael.com/japan-us-seek-to-up-pressure-after-north-korea-missile-launch/>.

16 Joshua Berlinger, Ben Westcott, "North Korea Missile Launch: Are US Options Diminishing?", *CNN Politics*, 29 August 2017, <http://edition.cnn.com/2017/08/29/politics/north-korea-japan-missile-what-next/index.html>

actions only increase the North Korean regime's isolation in the region and among all nations of the world.”¹⁷

At this point, it is important to consider the following questions:

- How has North Korea developed its capabilities from building copies of Russian missiles since the fifties, to build a road-mobile liquid propellant ICBM and have that missile threaten the continental US?¹⁸
- Is there any solution without the use of force and what kind of legal option may there be for halting NK's nuclear capacity and long-range missile deployments?



Sources: “As North Korea Builds up Missile Capabilities, Should Hawaii be Worried?”, <http://www.channelnewsasia.com/news/world/as-north-korea-builds-up-missile-capabilities-should-hawaii-be-8874932>

<http://www.channelnewsasia.com/news/world/as-north-korea-builds-up-missile-capabilities-should-hawaii-be-8874932>

In terms of resolution of current confrontation, the most rational resolution is considered to be an agreement between China, Russia and USA on a joint formula, with a new

17 “Trump issues warning to North Korea over missile launch”, The Australian, 30 August 2017, <http://www.theaustralian.com.au/news/world/japan-warns-about-north-korea-missile/news-story/7c7b072d6c6200a934da0d297d527a7c>.

18Ralph Savelberg: “This is Not the ICBM You Are Looking For; Detailed Analysis Of North Korean Missile”, Breaking Defense, 6 July, 2017, <http://breakingdefense.com/2017/07/this-is-not-the-icbm-you-are-looking-for-detailed-analysis-of-north-korean-missile/>.

study to be initiated by UN and IAEA on the future inspection mechanisms within the context of experiences. Therefore, in terms of preventing a possible nuclear attack, it is quite important to continue involving diplomatic methods, international law rules, legal agreements on non-proliferation for the resolution of conflicts, as well as the use of military deterrence factor.

North Korea's newest ballistic missile test has reintroduced debate at the highest levels of the Trump administration on how military force can be employed for stopping Kim Jong Un's advance of nuclear warheads and ballistic missiles. U.S. national security adviser H.R. McMaster told reporters stated that "for those who have said, and been commenting about a lack of a military option, there is a military option. Now, it is not what we would prefer to do. Within the same press briefing, UN Ambassador Nikki Haley accredited that *if sanctions and diplomatic pressure don't work, the UN may not be able to do much more. So, having said that, I have no problem with kicking it to (Defense Secretary) Gen. James Mattis because I think he has plenty of options*". During his speech at Joint Base Andrews, the Air Force installation outside Washington, President Donald Trump highlighted the strength of US military options. He did underline that "*After seeing your capabilities and commitment here today, I am more confident than ever that our options in addressing this threat are both effective and overwhelming*".¹⁹ Trump, maintaining that nuclear weapons and ballistic missiles held by North Korea to be threatening to the entire world with a possibility of an unthinkable loss of human life, and also declared to believe that Kim-Jong Un is a "Rocket Man...on a suicide mission". In this regard, he threatened that it may come to the point to "totally destroy" North Korea as the rogue nation, in his address in United Nations 71th General Assembly,²⁰

19 Barbara Starr: "Latest North Korea missile test renews US talk of military option", *CNN Politics*, 16 September 2017, <http://edition.cnn.com/2017/09/16/politics/north-korea-missile-test/index.html>.

20 Julian Borger: " Donald Trump Threatens to 'totally destroy' North Korea in UN Speech", *The Guardian*, 19 September, 2017, <https://www.theguardian.com/us-news/2017/sep/19/donald-trump-threatens-totally-destroy-north-korea-un-speech>.

North Korean missile over Japan



Source: AFP, 29 August 2017, <http://www.dailymail.co.uk/wires/afp/article-4831270/N-Korea-fires-ballistic-missile-Japan-Seoul-Tokyo.html>.

The UN Secretary General Mr. Guterres, underlined that millions of people were living in dread as a result of North Korea's nuclear and missile tests. "The use of nuclear weapons should be unthinkable," he said. "But today, global anxieties about nuclear weapons are at the highest level since the end of the Cold War."²¹

I think it's highly important to understand to discussion topic in this paper, why proliferation problem is so dangerous and new argument more than above mentioned "traditional deterrence theory". But what's even more important is the interest held by terrorist organizations, non-state actors, the proliferating nation states; such as North Korea, as discussed in this paper, and any individuals in demanding access to nuclear materials and weapons; and the possibility of them pursuing their interest through means defined as 'black market'; working with illegal arms manufacturers, transnational networks, shippers and traffickers, arms brokers and criminal organizations. An essential element of combating illicit trafficking must therefore involve an international control by IAEA. In order to prevent nuclear materials falling into the wrong hands or those of terrorist organizations, stronger international legal measures applicable for all states must be developed and employed to control and deter the illegal nuclear trafficking worldwide.²² Thirdly, alternately to military options, which holds only quite limited benefits; international law and diplomacy provides many preventive measures, and some combination of negotiations, mediation, containment,

21 "Trump: US Would Destroy North Korea if Forced to Defend Itself", BBC News, 19 September 2017, <http://www.bbc.com/news/world-us-canada-41324970>.

22 Mesut Hakkı Caşın:"Illicit Arms Trafficking Crime in International Law ", 5 th Traditional I Law Conference, University of Maribor, Slovenia, 2017, pp.34-57.

deterrence, sanctions, and eventual diplomacy are strictly preferable. In this point, some reassurance and establishment dialogue regulations between China and Russia could be established, with the nations having already been urged by the UN to tone down their rhetoric and start to establish dialogue with North Korea in order to achieve a solution.

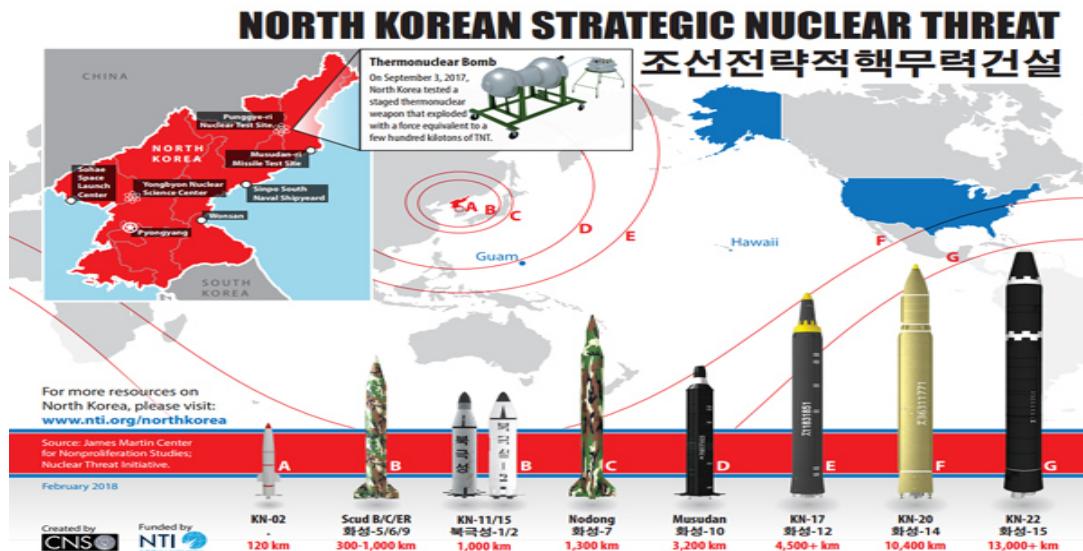
On August 4, 2018, the report prepared by a commission submitted to UN Security Council has stated that North Korea has not halted its nuclear and missile activities²³ which means the violation of UN sanctions. According to this report, Pyongyang has resorted to a "massive increase" of illegal ship-to-ship transfers of oil products and has been endeavouring to trade weapons overseas. North Korea has so far not remarked on the document's judgments. Before that, US officials did state that Pyongyang seemed to be constructing new ballistic missiles notwithstanding fresh warming up connections with US President Donald Trump's administration and initiates for the denuclearisation. Unnamed US officials would express the Washington Post that spy satellites had covered ongoing activity at a site that has manufactured ballistic missiles. It has been expressed in the latest UN report that "*North Korea] has not stopped its nuclear and missile programmes and continued to defy Security Council resolutions through a massive increase in illicit ship-to-ship transfers of petroleum products, as well as through transfers of coal at sea during 2018. Pyongyang also attempted to supply small arms and lights weapons and other military equipment via foreign intermediaries*" to Libya, Yemen and Sudan. *North Korea's activities had made financial sanctions ineffective*".²⁴ The report arose as US Secretary of State Mike Pompeo stated that he remained "optimistic" that North Korean denuclearisation possibly will be realized. Speaking ahead of a summit of the Association of South East Asian Nations (Asean) in Singapore, he mentioned that: "*The work has begun. The process of achieving denuclearisation of the [Korean] peninsula is one that I think we have all known would take some time. It was important to maintain "diplomatic and economic pressure" on North Korea to achieve "the final, fully verified denuclearisation. I had seen reports that Russia was issuing permits allowing North Koreans to work on its territory, defying the sanctions. I want to remind every nation that has supported these resolutions that this is a serious issue and something that we will discuss with Moscow. We expect the Russians and all countries to abide by the UN Security Council resolutions and enforce sanctions on North Korea*".²⁵ Russia has repudiated a report

²³ For more information on this issue please see, Mesut Hakkı Caşın, "Pasifik Bölgesinde Kuzey Kore ile ABD ve Müttefikleri Arasındaki Nükleer Krizin Tırmanma Tehdidi Bölgesel Ölçekte Bir Çatışmanın Habercisi Olabilir mi?", *Bilimevi Dış Politika*, Üç Aylık Fikir Dergisi (Ocak-Şubat-Mart 2018), Sayı:3, pp. 7-32 and Ozan Örmeci and Sina Kisacık, *Rusya Siyaseti ve Rus Dış Politikası: Teorik Çerçeve-Tarihsel Arka Plan-Örnek Olaylar*, (Ankara: Seçkin Yayıncılık, Haziran 2018), pp. 287-308.

²⁴ "North Korea continuing nuclear programme - UN report", *BBC News: Asia*, 4 August 2018, available at: <https://www.bbc.com/news/world-asia-45067681>, (Accessed on 19 September 2018).

²⁵ <https://www.bbc.com/news/world-asia-45067681>. Also please see, Nuclear Treaty Initiative, "Countries: Overview – North Korea", Last Updated: June 2018, available at:

by the Wall Street Journal that it stood permitting thousands new North Korean labourers into the country.



Source: <https://www.nti.org/learn/countries/north-korea/>.

According to International Atomic Energy Agency's latest report, as of August 22, 2018, Pyongyang remains enduring to improve its nuclear weapons programme which raises questions regarding the country's commitment to denuclearization.²⁶ In one of the most specific reports on Pyongyang's current nuclear activities, the International Atomic Energy Agency watched out actions constant with the enrichment of uranium and manufacturing at the country's key nuclear site.²⁷ The continuance and additional expansion of the DPRK's [North Korea's] nuclear programme and linked declarations by the DPRK are situated a reason for grave alarm.²⁸ At a historic summit between Donald Trump and Kim Jong-un in Singapore in June, the US president and North

<https://www.nti.org/learn/countries/north-korea/>, (Accessed on 19 September 2018), "North Korea has not stopped nuclear, missile programme according to confidential UN report", *The Telegraph: News*, 4 August 2018, available at:

<https://www.telegraph.co.uk/news/2018/08/04/north-korea-has-not-stopped-nuclear-missile-programme-according/>, (Accessed on 19 September 2018).

²⁶ Benjamin Haas, "North Korea is still developing nuclear weapons, says IAEA", *The Guardian: North Korea*, 22 August 2018, available at:

<https://www.theguardian.com/world/2018/aug/22/north-korea-still-developing-nuclear-weapons-iaea-report-un>, (Accessed on 19 September 2018).

²⁷ For more detailed info on this issue please see, International Atomic Energy Agency Board of Governors General Conference, "GOV/2018/34-GC(62)/12, Application of Safeguards in the Democratic People's Republic of Korea Report by the Director General - Date: 20 August 2018", available at: https://www-legacy.iaea.org/About/Policy/GC/GC62/GC62Documents/English/gc62-12_en.pdf, (Accessed on 19 September 2018).

²⁸ "North Korea's nuclear programme has not been halted, says UN", *The Guardian: North Korea*, 4 August 2018, available at: <https://www.theguardian.com/world/2018/aug/04/north-koreas-nuclear-programme-has-not-been-halted-says-un>, (Accessed on 19 September 2018).

Korean leader settled to make efforts for the “thorough denuclearization” of the Korean peninsula. But experts have cautioned that lacking a formal deal between the US and North Korea, Kim would carry on advancing his nuclear and missile programmes. For Duyeon Kim, an adjunct senior fellow at the Center for a New American Security, “*The Singapore summit wasn’t a nuclear deal and there’s no agreement between Washington and Pyongyang that would encourage North Korea to act any differently. Negotiating with North Korea is always going to be a long, bumpy and twisty process, and they are savvy negotiators. They want to hold on to their nuclear weapons as long as possible while extracting as many concessions along the way. A nuclear inventory will always be imperfect. North Korea will never give a complete accounting because they want cards in their hand and to maintain some degree of leverage*”.²⁹



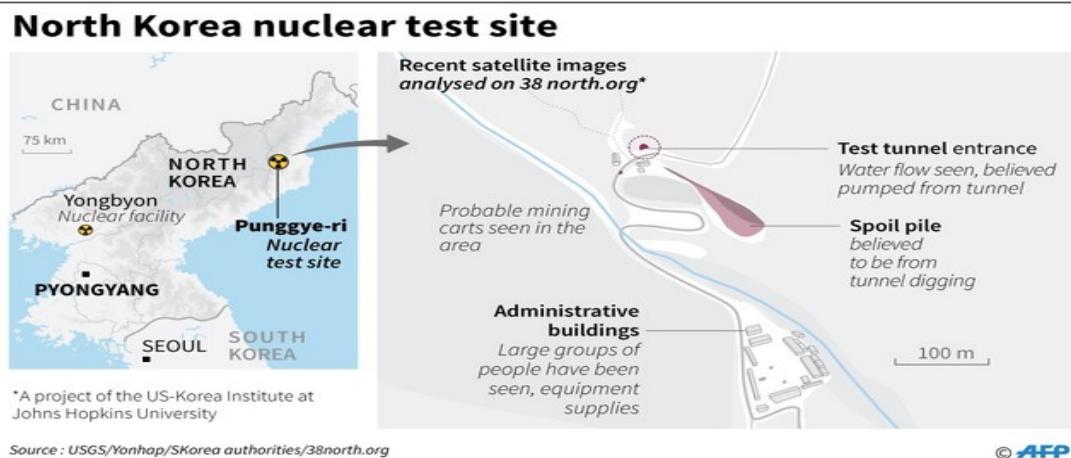
Source: <http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2928738>.

In parallel with these developments, as of August 25, 2018, U.S. President Donald Trump has postponed State Secretary Mike Pompeo's planned visit Pyongyang. Trump has stated that “*I have asked Secretary of State Mike Pompeo not to go to North Korea, at this time, because I feel we are not making sufficient progress with respect to the denuclearization of the Korean Peninsula,*” Trump tweeted on Friday. “*Secretary Pompeo looks forward to going to North Korea in the near future, most likely after our Trading relationship with China is resolved*”.³⁰ A senior diplomatic source spoke CNN that State Department officials were there for “briefing allies’ embassies about their purposes for the trip like 10 minutes before the trip was cancelled. Adam Mount, senior fellow and director of the Defense Posture Project at the Federation of American Scientists, has mentioned that “*The President’s tendency to undercut his negotiating team has made it easy for Pyongyang officials to refuse their demands. Now, as the administration finally installs a negotiating team, the President signals publicly that he*

²⁹ <https://www.theguardian.com/world/2018/aug/22/north-korea-still-developing-nuclear-weapons-iaea-report-un>.

³⁰ Zachary Cohen and Jeremy Diamond, “Trump says Pompeo won’t go to North Korea, criticizes denuclearization progress”, CNN: Politics, 25 August 2018, available at: <https://edition.cnn.com/2018/08/24/politics/trump-pompeo-north-korea/index.html>, (Accessed on 19 September 2018).

doubts their ability to make progress. Washington has allowed talks to drift along, unstable, unproductive, and without a coordinated negotiating team. It appears the President is willing to allow this to continue into the fall". On the other hand, a diplomatic source articulated CNN that while it remains thinkable those high-ranking officials in Seoul were informed of Trump's decision to call off the trip earlier, the statement trapped South Korean diplomats at the working level off guard. South Korean President Moon Jae-in plans for meeting Pyongyang next month for a third summit with Kim.³¹



Source: <https://www.dailysabah.com/asia/2017/05/04/north-korea-resumes-activity-at-nuclear-test-site>.

On September 19, 2018, South Korean President Moon Jae and North Korean President Kim Jong-un would convene in Pyongyang. After this summit, several agreements have been signed between South Korea and North Korea. The deal in military sphere was contracted by South Korean Defense Minister, Song Young-moo, and North Korean Defense Minister of People's Armed Forces, No Kwang Chol in the attendance of the two states' leaders. According to the joint declaration by the leaders, North Korea has decided to completely disassemble its rocket testing field in Tonchkhani and will allow international observers in order for visiting the area. Moreover in the same declaration, it has been stated that North Korea was going to disassemble its nuclear reactor in Yonbyon within the context of settlements with U.S. In the aftermath of the summit, North Korean leader has pledged to visit Seoul in near future. He has too mentioned that both nations have decided to make efforts for the denuclearization of the peninsula. In the meantime, South Korean president has stated that Seoul and Pyongyang have decided to eliminate danger of war on Korean Peninsula. The joint statement has too pointed out that the works on linking of roads and railways between the two nations would begin prior to 2019. Seoul and Pyongyang have likewise decided to send joint team to 2020 Olympic Games plus to yield to joint submission to host 2032 games. Furthermore, the two nations have settled to terminate large-scale artillery exercises and military flights nearby demarcation line. They have too settled to take out servicemen from the demilitarised zone and disarm personnel

³¹ <https://edition.cnn.com/2018/08/24/politics/trump-pompeo-north-korea/index.html>.

in Panmunjom truce village. Two Koreas have settled to form 80-kilometre zone free from military exercises in Yellow Sea, Sea of Japan.³² This summit has been welcomed by the Russian Federation. Russian Ambassador to North Korea Alexander Matsegora has evaluated the importance of this meeting as follows;

"We view the meeting between the two leaders of North and South Korea as purely positive. Reconciliation between the two parts of the Korean Peninsula is exactly what will help to ease tensions, create an atmosphere of mutual trust, mutual consideration for the interests of each other, and, consequently, this will lead to reduction of military tensions. The United States' accusations that Russia is "cheating" on the UN Security Council (UNSC) resolution on North Korea are unfair. They are not based on facts, but on speculations and assumptions that are groundless. Russia scrupulously, very responsibly and consistently fulfills the requirements of the resolutions of the UN Security Council. Almost 20,000 [North] Korean workers have left Russia. And they continue to leave. By the end of the year we will not only 'fulfill,' but 'outperform' the requirements provided for in the UNSC resolution, the number of North Korean citizens working in our country will be halved".³³



Source: <https://www.bbc.com/news/world-asia-45569924>.

On September 17, 2018, US Ambassador to the United Nations Nikki Haley indicted Russia of “steady” violations of the UN Security Council resolution regarding the

³² “DPRK, South Korea Sign Military Agreement Following Summit in Pyongyang”, *Sputnik International: Asia & Pacific*, 19 September 2018, available at: <https://sputniknews.com/asia/201809191068152005-north-south-korea-will-sign-agreement/>, (Accessed on 19 September 2018).

³³ “Russia Welcomes Inter-Korean Summit – Ambassador to North Korea”, *Sputnik International: World*, 19 September 2018, available at: <https://sputniknews.com/world/201809191068154454-inter-korean-summit/>, (Accessed on 19 September 2018).

sanctions against Pyongyang, including limitations on supplies of fuel to North Korea and hiring North Korean workers. She has stated the following remarks on this issue;

"Russia must cease its violations of North Korea sanctions. It must end its concerted effort to cover up evidence of sanctions violations. When North Korea assassinated Kim Jong Nam with VX, a deadly nerve agent, the United States moved to strengthen UN controls of the flow of chemical and biological weapons technology of North Korea," she told the UN Security Council. "Russia... turned around and again blocked the sanctions committee from updating its 12-year-old sanctions list".³⁴

On September 19, 2018, Russia's ambassador to North Korea, Alexander Matsegora, have assumed that the US assertions that Russia remained "violating" on the UN Security Council (UNSC) resolution on North Korea were absolutely unjustified and that the state strictly act in accordance with its commitments. Russia's ambassador to North Korea, Alexander Matsegora has defined them "unfair", who underlined that they were not grounded on evidences, but rather counted on unfounded speculations and assumptions. Matsegora has too underscored that Russia "scrupulously, very responsibly and constantly" fulfills the obligations of the resolutions of the UN Security Council and also highlighted that *"this was the reason why bilateral trade between Russia and North Korea fell by more than 70 percent since the beginning of the year".³⁵* With regard to this issue, Russian Ambassador to the United Nations Vassily Nebenzia has rejected American allegations and has responded to these claims as follows: *"Russia refutes the claims made by the United States that Moscow has breached the sanctions regime against North Korea. On the Patriot oil tanker, the group of experts themselves said the ship was not in violation of the sanctions regime".* In line with these statements, Russian Deputy Foreign Minister Igor Morgulov has assumed that Russia will appeal to other Security Council countries to ease sanctions on North Korea as the country takes steps on the way to denuclearization.³⁶

In parallel with the significance of this summit between North Korea and South Korea, Simone Chun, fellow at the Korea Policy Institute and member of the Korean Peace Network, has underlined the following issues with regard to the rapprochement initiatives between these two states:

³⁴ "Russia Denies US Accusations of Violating North Korea Sanctions - UN Ambassador", *Sputnik International: World*, 17 September 2018, available at: <https://sputniknews.com/world/201809171068103700-haley-us-russia-north-korea/>, (Accessed on 20 September 2018).

³⁵ "Moscow Regrets US Attempt to Control UNSC Regarding N Korea Sanctions Issue", *Sputnik International: World*, 19 September 2018, available at: https://sputniknews.com/world/201809191068170235-russia-us-accusations-north-korea-sanctions/?utm_source=push&utm_medium=browser_notification&utm_campaign=sputnik_inter_en, (Accessed on 20 September 2018).

³⁶ <https://sputniknews.com/world/201809171068103700-haley-us-russia-north-korea/>.

"It's very disappointing that as President Moon Jae-in is making another very historic summit... that there" many disagreements within the Trump administration on what to do with North Korea and US negotiations. This is, again, Moon Jae-in taking the initiative. We should really be supporting the peace process and really counter the opposition and conflicting messages coming from the Trump administration. Diplomacy will render better results. North Korea has done several irreversible steps toward denuclearization and respecting and implementing the Singapore summit, whereas the United States has so far only done one by suspending the war games. I really think the United States should take reciprocal action and show commitment. There's a good chance [that Moon and Kim could sign a peace agreement], however, I know that President Moon Jae-in is still very [interested] in working with the United States. I don't think that they'll sign a peace treaty".³⁷

On the other hand, another evaluation on this issue has come from Jung H. Pak, SK-Korea Foundation Chair in Korea Studies Senior Fellow - Foreign Policy, Center for East Asia Policy Studies. Pak has stressed the importance of following issues with regard to this question:

"Calling for peace talks is not a new tactic. The regime has used it in the past to delay and deflect attention from the nuclear issue. Yet while Kim Jong-il, the current leader's father, probably recognized that this was a maximalist position and that the United States would not accept peace talks in the absence of a nuclear agreement, Kim Jong-un probably has a plausible reason to believe that an end of war declaration is within his grasp with President Trump. He sees a potentially once-in-a-lifetime opportunity with President Trump, who has openly derided the value of the U.S. alliance with South Korea. In Trump, Kim has a sympathetic partner in the White House who held a summit with him against the counsel of his advisers, and agreed to a statement at Singapore, which by all measures was weak and failed to advance the U.S. policy of final, fully verified denuclearization. Second, unlike the conservative Lee Myung-bak and Park Geun-hye administrations, which took a hard line against the Kim regime, Kim Jong-un now has a partner in Seoul with the progressive Moon administration. Since Kim offered an olive branch in his New Year's speech, President Moon has brokered, nurtured, and prodded U.S.-North Korea talks, in large part to empower his push for greater inter-Korean engagement. Kim and Moon have expressed their mutual desire for pan-Korean autonomy in Korean Peninsula affairs and relatively downplaying the nuclear issue. Third, Kim seeks to maintain the initiative on shaping the global debate about how to approach the North Korea problem. That is, he is looking to shift the discussion to non-nuclear

³⁷ "US Must 'Show Commitment' to Peace Talks with North Korea – Scholar", *Sputnik International: Opinion*, 19 September 2018, available at: <https://sputniknews.com/analysis/201809191068150156-kim-moon-meeting-pyongyang-trump-administration/>, (Accessed on 19 September 2018).

issues to deflect attention away from its nuclear weapons and dampen the international community's appetite for implementing sanctions. After declaring that he has completed the nuclear weapons program, Kim has pivoted toward engagement and focusing on the economy—key themes in the recent parade held last week to celebrate the 70th anniversary of the country's founding. The past nine months of summity have revived and sustained calls for further engagement, even as Pyongyang continues to reject timelines and verification measures for denuclearization and covertly make additional progress on its strategic programs. Finally, Kim is probably seeking to reduce his dependence on China by trying to start the process for peace negotiations with the United States. Kim might be calculating that sustained bilateral talks with Washington would increase his leverage against Beijing and stimulate Chinese leaders to be more pliable to Pyongyang's preferences—such as reducing sanctions implementation—by taking advantage of Chinese concerns about being sidelined in Korean Peninsula issues".³⁸



Donald J. Trump @realDonaldTrump

North Korean Leader Kim Jong Un just stated that the "Nuclear Button is on his desk at all times." Will someone from his depleted and food starved regime please inform him that I too have a Nuclear Button, but it is a much bigger & more powerful one than his, and my Button works!

1/2/18, 6:49 PM

Source: <https://www.cfr.org/timeline/north-korean-nuclear-negotiations>.

Moreover, Pak has highlighted some important issues regarding this question as follows:

"As the White House prepares for another summit in which the end-of-war declaration almost certainly will be discussed, the Trump administration must be thoughtful about Kim's motivations. The declaration—despite what Kim might say in the next meeting—is not a panacea and it is probably not the pivot on

³⁸ Jung H. Pak, "The real reason Kim Jong-un wants to declare an end to the Korean War", *Brookings Series: Trump and Asia Watch – Order from Chaos*, 17 September 2018, available at: https://www.brookings.edu/blog/order-from-chaos/2018/09/17/the-real-reason-kim-jong-un-wants-to-declare-an-end-to-the-korean-war/?utm_campaign=Brookings%20Brief&utm_source=hs_email&utm_medium=email&utm_content=65988763, (Accessed on 19 September 2018).

which the future of U.S.-North Korea ties, regional and global stability, and North Korean denuclearization rests. While a declaration might buy us some time of relative quiet, it would set the stage for bigger problems down the road. There are serious risks of a premature peace declaration. It would reward Pyongyang for taking cosmetic, reversible actions, further legitimize North Korea's claimed status as a nuclear weapons power, erode the U.S.-South Korea alliance and U.S. credibility in the region, and weaken global non-proliferation norms. It would also serve as a potential tool for Pyongyang to wield down the line when military exercises resume or Washington announces additional sanctions. Pyongyang is also likely to use Washington's "hostile" actions as justification if the North Korean regime decides to conduct more nuclear and ballistic missile tests to put the onus on the United States for not living up to the peace declaration. Perhaps most importantly, Kim's confidence about his ability to manage the consequences of his bad behavior is likely to grow, potentially making him even more willing to take risks in the future and increasing the potential for miscalculation that quickly spirals into a military conflict. Ultimately, the case for U.S. agreement to a peace declaration depends on the key assumption that Kim's idea of peace is linked to his relinquishing of nuclear weapons. Instead, the history of North Korea's nuclear ambitions, the ideological infrastructure that the Kim dynasty has built over the decades, and the regime's own public statements strongly suggest that peace—from North Korea's perspective—is achievable because it has nuclear weapons. Any planning for an end-of-war declaration must confront this important distinction and prepare for the consequences as the North Korea nuclear issue continues to evolve".³⁹



³⁹ https://www.brookings.edu/blog/order-from-chaos/2018/09/17/the-real-reason-kim-jong-un-wants-to-declare-an-end-to-the-korean-war/?utm_campaign=Brookings%20Brief&utm_source=hs_email&utm_medium=email&utm_content=65988763.

Source: <https://www.voanews.com/a/Korea-sanctions/4577831.html>.

Regarding the recent rapprochement initiatives between Seoul and Pyongyang, John Dunn, professor emeritus of political theory at Cambridge who has a long-standing interest in the politics of the Korean Peninsula, has shared his views on this issue in his interview with Sputnik International as follows;

"I think there will be a lot of statements about how good it will be for relations; there will be a few practical proposals about how to make them a bit closer in different ways. It's possible that there will be some subsequent relations between the North Korean leader and the United States. I don't see much chance of that shifting the basic shape of the problem, but it's really important for the South Korean leader and, actually, it's very important for the North Korean leader for relations between the South and the North to improve and for there to be less of a sense of immediate prices. Unfortunately that doesn't actually deal with the major issue, which is North Korean nuclear weapons. I don't really see there's much the South Korean leader can do to shift that; that depends entirely on the approach of the North Korean leader. I don't think he will be persuaded to alter his approach by either the South Korean leader or President Trump. I don't think that this actually can be shifted much from South Korea, that's the main point I wanted to make. I think it's entirely a game between North Korea and the United States. One way of thinking is that it's essentially a game between the North Korean leader and Trump; the timing of this game is very strongly connected to the American domestic political process and the imminence of congressional elections. I don't think it has been possible for North Korea to abandon nuclear weapons; I don't think there's anything that the US could offer North Korea which would make it reasonable for them to abandon nuclear weapons. So, I think that it's a stuck situation, as it's been for a long time. I don't think that North Korea means to denuclearize, that's a pretty fundamental sort of difficulty. The reason I don't think it means to do it is because it doesn't have a good reason to. The only good reason it could have would be the fear of an immediate US attack and I think that it's very unlikely that that will occur now. It was a little bit likely that it would occur early around in the Trump administration although we don't, obviously, know how likely it was. I don't think it's likely to occur now because it would make Trump look like a complete imbecile apart from anything else and I don't think he wishes to look a complete imbecile at the moment. For a bit it looked as though he'd really pulled off a great coup; that was always a mirage, but it looked good and it's very important for him to go on looking good. It's clear by now that it's much more important for him to go on looking good than anything else at all. And I think it would be utterly bizarre for him to order an attack on North Korea. The diplomatic game between Kim and Trump will go on as long as Trump is president and what shape it will take in the second half of Trump's first

presidency will depend very much on what happens in congressional elections".⁴⁰

2. Extremists' and Other Non-State Actors' Potential Nuclear Terrorism Threat and To Keep Nuclear Facilities Security

It is known that terrorism has a long background which it always posed threat to human life and universal civilization values. While Maximilien Robespierre, a frontrunner in the French Revolution, declared in 1794 that "terror is nothing other than justice, prompt, severe, inflexible," Walter Laqueur defined terrorism as being "the use or the threat of the use of violence, a method of combat, or a strategy to achieve certain targets... [I]t aims to induce a state of fear in the victim that is ruthless and does not conform to humanitarian rules... [P]ublicity is an essential factor in the terrorist strategy."⁴¹ Comprehending the actual risk of nuclear terrorism necessitates comprehensive and possibly multidisciplinary examination of both probable terrorist motivations, intentions as well as their potential technical capacities.⁴²

Yes, terrorism is an ancient criminal tactic and strategy, but will be more dangerous and deadly because of the availability of nuclear weapons. The danger may continue to grow until the point that it is a threat to nations, governments, and people everywhere, and require a response involving cooperation to secure a peaceful present and future for our planet. The threat of nuclear and radiological terrorism remains one of the greatest challenges to international security, and the threat is constantly evolving. The purpose of the nuclear security regime is to prevent, detect and respond to nuclear security events, even illicit trafficking of nuclear material or a terrorist nuclear attack. New academic arguments must be developed and reasonable answers should be found to why terrorist organizations are diligently trying to acquire nuclear materials. There are some arguments that land-based assaults, deliberate aircraft crashes, and other terrorist acts like 'Fukushima-style' disasters may be staged by terrorist groups, or that these groups may use new technology to attempt attacks, or steal nuclear material in order to make a nuclear "dirty bomb". Of course, terrorist groups to make a crude bomb is very difficult yet not impossible, since their aim is to use advanced technologies such as using cyber-terrorism which targets vulnerabilities in the reality of today. Any possibility of a small nuclear explosion in a major city would

⁴⁰ "North Korea Can't Abandon Its Nuclear Weapons – Scholar", *Sputnik International: Opinion*, 19 September 2018, available at: <https://sputniknews.com/analysis/201809191068162261-north-korea-nuclear-weapons/>, (Accessed on 20 September 2018).

⁴¹ Walte Laqueur: "*The Age of Terrorism*", Boston, Little & Brown, 1987, p. 143.

⁴² Morten Bremer Maerli, Annete Schaper, Frank Barnaby: "The Characteristics of Nuclear Terrorist Weapons", *American Behavioral Scientist*, Vol. 46, No. 6, February 2003, p.728.

immediately kill tens of thousands of people and a bigger explosion would cause even more fatality.

General opinion about the terrorist organizations' criminal motivations can employ a range of tactics to achieve their goals, including the use of conventional weapons, hijackings, including suicide bombings, explosives, and guns. However today, which a more chaotic structure than that of Cold War is present, there is strong concern that terrorists may use nuclear or other radioactive material to commit an act of terrorism. The risk of nuclear terrorism may still be low, but the possible level of physical destruction, fatalities, and injuries is so great, that in itself warrants serious consideration against the potential acquisition and use of nuclear devices by terrorists. Nuclear threats and consequences of nuclear terrorism transcend international borders. Opinions about the threat of nuclear terrorism differ among scholars and security experts.

1. Terrorists could acquire a nuclear weapon.
2. Nuclear terrorism is unlikely to realize such a strenuous goal. In that sense, the lack of nuclear terrorism so far is more related "...to the absence of tools rather than absence of motivation." For some, the threat of nuclear terrorism remains as "an exaggerated nightmare." Some do not accept the danger of large-scale nuclear terrorist violence in USA due to the domestic factors; namely geography, politics and security policy. Also, the conventional tools will probably continue serving as the weaponry of choice for many terrorists. The results of conventional arming, which was painfully experienced on September 11, 2001, could still prove to be more effective in terms of realization of terrorist goals. Furthermore, there will stand for practical, strategic and even moral limitations towards uses of Weapons of Mass Effects (WMEs). The limitations towards the use of WMEs stay for especially severe for the terrorists who are related with their fellow citizens such as social revolutionary and national secessionist terrorists. Conventional off-the-shelf armament and well-known manners stand for therefore probably to endure fundamental means for many terrorists.⁴³

On the other hand, we must underline that there is important difference between the states and non-state actors to have nuclear weapons. States are directly obliged under international law and nonproliferation treaties. Any violation of the nuclear agreements by the states, may be answered with heavy legal, political, even military sanctions, embargoes and arms export controls. Conversely, these repercussions may not be effective against terrorist organizations. The main threat is the procurement of nuclear weapons of these terrorist groups to be used in order to realize their illegal political-ideological purposes.

43 Maerli, Schaper, Barnaby: "The Characteristics of Nuclear Terrorist Weapons", 2003, Vol. 46, Issue, p.728.

- Does international community have enough security and safety standards of physical protection against a terrorist theft?
- Can we eliminate and deter non-state actors from purchasing a nuclear weapon or materials necessary to make a nuclear bomb device?

New international organizations, such as the World Institute for Nuclear Security (WINS), will need to play an absolutely critical role in promoting best physical security practices between the existing nuclear power states and new states that construct nuclear power plants. Understanding the real threat of nuclear terrorism requires in-depth and probably interdisciplinary analysis of both possible terrorist motivations and intentions, and of their potential technical capabilities as modern terrorism employs criminal actions with advanced technology networks such as cyber-attacks and their violence capacity is currently enlarging to span across the globe, causing increased instability. Thus, today's terrorist groups are increasingly interested in massive and violent destruction. For these new terrorists, nuclear weapons are perfect for the purpose of inflicting massive destruction as well as augmenting their power and prestige. Determining their motivations will be more difficult in some cases than in others.⁴⁴ The reality is that there are a number of factors that could affect nuclear materials; technologies and know-how are more widely available today than ever before. Academic scholars typically have been classifying nuclear and radiological terrorism into four threat categories.

First, a non-state actor such as a terrorist or criminal or a group of terrorists or criminals could acquire a nuclear weapon from an arsenal of a nuclear-armed state. In order to manufacture a crude nuclear weapon, a terrorist organization needs to possess specialized expertise in areas such as high explosives, propellants, electronics, nuclear physics, chemistry and engineering. Knowledge of the physical and chemical properties of plutonium or highly enriched uranium (HEU) is essential.

The type of nuclear explosive device that a terrorist group might assemble depends primarily upon the type and quantity of fissile material that it can obtain. Each type of device has its advantages and disadvantages. Al Qaeda and other terrorist groups are determined, as President Obama stated, "to buy, build or steal" a nuclear weapon and "would have no problem with using it." According to President Obama, if terrorist organizations are to possess nuclear weapons, this will be a threatening "game changer." But if non-state terrorist groups were to buy, steal, or build a bomb, a state would be involved -either as the source of the weapon, or the fissile material required in the production. The countries of primary concern with respect to the transfer or theft of nuclear weapons are all at inflection points.

⁴⁴ Bonnie Jenkins, "Combating Nuclear Terrorism: Addressing Non-state Actor Motivations", *The Annals of the American Academy of Political and Social Science*, Vol. 607, *Confronting the Specter of Nuclear Terrorism*, September 2006, pp. 33-42.

With regard to the first point, it is sometimes speculated that a state might actively or passively help a terrorist group to acquire a nuclear weapon. The possibility that a terrorist weapon could be traced back to the sponsor, even if relatively low, should still be too high in relation to the worst possible consequences – nuclear annihilation – for a state to sponsor or even knowingly to host nuclear terrorists.⁴⁵ Nuclear terror would cause death and economic damage in a magnitude previously unknown outside major war. Market conditions are favorable for the transfer of nuclear weapons to terrorists. In the 1990s alone, Aum Shinrikyo, a doomsday cult, sought to hire Russian scientists and students to build a nuclear weapon, Al Qaeda spent \$3 million in attempts to obtain Russian fissile material and build a bomb, Czechoslovakia seized 3 kilograms of highly enriched uranium (HEU) from a car in Prague (probably smuggled from a research institute near Moscow), and a former Russian general announced that several dozen suitcase bombs had disappeared. In the first five years after 2000, the Taliban was caught seeking to hire Russian nuclear scientists; terrorists were seen reconnoitering Russian nuclear warhead storage sites.⁴⁶

The second nuclear threat is the possibility of the manufacturing of a non-state actor to build an improvised nuclear device (IND) after the retrieval sufficient fissile material such as highly enriched uranium (HEU) or plutonium. Many nuclear materials can be exported for beneficial uses as well as for the creation of weapons, so called dual-use materials. This option basically concerns determining the source of the bomb itself. Terrorist groups should combine fissile-material and bomb fragments, which would reveal components or impurities, including tritium, U-240, neptunium, americium, gadolinium, curium and promethium, found in the plutonium or HEU core of the weapon. If we evaluate criminal attempts in terms of successfully stealing a significant amount of plutonium or highly enriched uranium (HEU) would certainly remove the greatest barrier faced by terrorists in achieving their goal of obtaining a nuclear weapon. In order to prevent possibility of illegal trafficking nuclear material, of spent fuel is also unlikely since it is extremely radioactive and can be handled only with special modern secured storage equipment and advanced dual shielding mechanism.

A third possibility is that terrorists will sabotage a nuclear facility, releasing radioactive material over a wide area. In this manner, the plutonium device, when detonated, does not result with a significant nuclear explosion, the explosion created by chemical high explosives would spread the plutonium widely, principally in the form of powder. If an inflammable element namely an aluminum-iron oxide (thermite) were brought together with the high explosives, the explosion would be emerged with a severe fire. A high amount of the plutonium represents probably to endure un-fissioned and would be spread with the explosion or volatilized through the stern heat. Much of the plutonium stands for probably be spreading in that way as small parts of plutonium dioxide taken

45 Robin M. Frost: "Terrorism and nuclear deterrence", *The Adelphi Papers*, Vol.45, No: 378, 2006, pp.63-68.

46 Anders Corr: "Deterrence of Nuclear Terror", *The Nonproliferation Review*, Vol. 12, No: 1, 2011, pp.127-14.,

up into the atmosphere in the form of fireball and scattered far and wide downwind.⁴⁷ Radioactive contamination poses threat through local contact, and might have additional powerful psychological effects on the victims. A great fraction of components stand for probably less than 3 microns in diameter and could, thus be breathed into and retained by lungs. In that sense, the victims might end up with lung cancer through exposure to the surrounding tissue with alpha particles. When they are spread to the environment, the plutonium dioxide stays for insoluble in rainwater and would remain in surface dusts and soils for a long time. The half-life of plutonium isotope plutonium-239 is 24.400 years. These factors would come together to solidify a huge component of an exposed city uninhabitable until it is decontaminated, which is an extremely costly procedure that may continue for a long time. The added threat of spread of many kilograms of plutonium turn out a crude explosive tool into a specifically attractive arm for terrorists, accompanied by the danger increased with the general population's fear regarding radioactivity.

The last possibility is cyber-attack. States and non-state actors, being the terrorist organizations in the first place, may use cyber-infrastructures for the purposes of stealing know-how from highly developed nuclear facilities, and/or merely for destructing a certain country's facility, as was the case in "Stuxnet"⁴⁸ that was created and used against Iranian nuclear advancement. These kind of malicious worms are possible to be created and use against possible nuclear targets.⁴⁹ Ongoing electronic high technologies and nuclear facilities have becomes ever more digitalized, the frequency of cyber-attacks, and the cost they incur, will continue to increase. A successful terrorist cyber-attack on a nuclear facility anywhere would have global consequences. Recent high-profile cyber-attacks, including the deployment of the sophisticated 2010 Stuxnet worm, have raised new concerns about the cyber-security vulnerabilities of nuclear facilities. As cyber-criminals, states and terrorist groups increase their online activities, the fear of a serious cyber-attack is ever present. This is of particular concern because of the risk – even if remote – of a release of ionizing radiation as a result of such an attack. Moreover, even a small-scale cyber-security incident at a nuclear facility would be likely to have a disproportionate effect on public opinion and the future of the civil nuclear industry.⁵⁰ Thus, after Cold War era cyber-

⁴⁷ Morten Bremer Maerli, Annette Schaper, Frank Barnaby: "The Characteristics of Nuclear Terrorist Weapons", *American Behavioral Scientist*, Vol. 46, No. 6, February 2003, pp. 735-736.

⁴⁸ Bruce Schneier: "The Story Behind the Stuxnet Virus", *Forbes*, 10 July 2010, <https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html>.

⁴⁹ Joseph Menn, "Exclusive: US tries Stuxnet-style campaign against North Korea but failed", *Reuters*, 29 May 2015, <http://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529>

⁵⁰ Caroline Baylon with Roger Brunt and David Livingstone: "Cyber Security at Civil Nuclear Facilities -Understanding the Risks", *Chatham House Report*, Chatham House, September 2015,

terrorism attacks have on rise mode. Today, many states take these concerns seriously and remain alert about possible cyber-terrorist attacks even non state actors.

- How can the possible terrorist cyber-attacks against to nuclear plants threats be reduced?
- What international community more urgent steps could be done?
- What kind of emergency measures operate if terrorists gained access to a reactor?

Considering a rapid cyber-attack threat, maintaining nuclear safety and physical security of the nuclear facilities would require the update and modernization of multi layered security measures to increase prevention capacities, yet the global shortage of technical experts pose a problem. There have been a number of reported incidents of cyber interference in nuclear power plants. These three publicly known attacks against nuclear plants are:

- Monju NPP (Japan 2014)
- Korea Hydro and Nuclear Power plant (S. Korea 2014)
- Gundremmingen NPP (Germany 2016).

Indeed, just after Gundremmingen nuclear power plant in Germany was hit by a “disruptive” cyber-attack, IAEA Director Yukiya Amano stated, “*This issue of cyber-attacks on nuclear-related facilities or activities should be taken very seriously. We never know if we know everything or if it's the tip of the iceberg.*”⁵¹ Notwithstanding important recent steps taken by the International Atomic Energy Agency (IAEA) to improve cyber-security across the sector, the nuclear energy industry currently has less experience in this field than other sectors. The IAEA, in pursuit of helping nations to build national cyber-warfare capabilities, has formulated both legal and technical guidelines.⁵² We can ask a critical question about how the effects of a possible nuclear terrorist attack will be. Some experts say any a crude nuclear device detonation by a terrorist group would result in an unprecedented number of casualties. A nuclear explosion would also create considerable fallout, potentially contaminating large areas. Beyond the immediate physical damage caused by a nuclear terrorist attack, the psychological, economic and sociological impacts of such an attack would be

https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylorBruntLivingstone.pdf.

51 Pierluigi Paganini: “Shocking, a German Nuclear Plant Suffered a Disruptive Cyber Attack”, *Security Affairs*, 10 October 2016,
<http://securityaffairs.co/wordpress/52116/security/nuclear-plant-attack.html>.

52 The Office of Nuclear Security was created in 2002 and the Technical Guidance on “Computer Security at Nuclear Facilities” (2011) has brought together “the knowledge and experience of specialists, who have applied, tested and reviewed computer security guidance and standards within nuclear facilities”. Since safety and security of nuclear facilities are sole responsibilities of sovereign nations, the IAEA and other multilateral initiatives extend only advisory help. See, Sitakanta Mishra:“Cyber Threat to Nuclear Installations”, http://www.claws.in/images/journals_doc/SW%20i-10.10.2012.130-133.pdf.

devastating. Unlike natural disasters, a nuclear attack may occur without warning, leaving little chance for preparation. An attack in an urban area would not only kill large numbers of people, it also could render the area virtually uninhabitable for a long period of time.⁵³

Even more fundamental, nuclear **terror would cause death and economic damage** of a magnitude previously unknown outside major war. Thus, if terrorists target extremely complex nuclear energy plants how to trigger readiness plan this kind of hidden threat that there are no easy answers. Many believe today that additional states, as well as non-state actors, will obtain a nuclear weapon capability or nuclear weapons, and that these weapons are more likely to be used than in the past. So-called rogue states are seen as irrational, and possibly as undeterable.⁵⁴ With HEU, gun-type bomb – like the one which obliterated Hiroshima – very plausibly within capabilities of sophisticated terrorist group. In contrast, a radiological dispersal attack would probably be less violent, but could significantly contaminate an urban center, causing economic and social disruption. Both types of attacks would have significant psychological impacts on the entire population. These two nuclear terrorism threats possess low probability, in that they are unlikely to occur due to the relatively high security for nuclear weapons and most fissile material, but they are very high consequence because of the massive destruction that would occur if a non-state actor could detonate one or more nuclear weapons or INDs on one or more cities. Why is this so remarkable? First argument is that a possible nuclear terrorism encompasses a spectrum of threats—the detonation of a nuclear bomb, an attack on a civil nuclear installation, or the dispersal of radiological materials through a “dirty bomb.” Each differs in probability and consequence.

Do we have the adequate mechanism to assure the security of nuclear facilities? Preventing the proliferation of nuclear materials and weapons is an important challenge to national and global security. The main goal of "non-proliferation regime" is, of course, the international safeguarding of fissionable material, partly ensured by inspections of nuclear reactors. On the other hand, we will shortly explain that there are large nuclear power plants or other facilities may strike as tempting targets to saboteurs, while nuclear materials may be stolen for use in nuclear or radiological weapons. The real weak link in security is, however, the transportation of plutonium, another reason why widespread nuclear electricity generation using this material is inadvisable. Transport necessarily involves removing material from fixed, large-scale facilities with highly regularized security into outside world and into environments that require transport by road, rail and sea, where there is less predictability in terms of

53 Kevin O'Neill, “The Nuclear Terrorist Threat”, August 1997, Institute for Science and International Security,

<http://www.isis-online.org/publications/terrorism/threat91301.pdf>.

54 Joseph F. Pilat, “The End of the NPT Regime?”, *International Affairs*, Vol. 83, No. 3, Thinking About 'Enlightenment' and 'Counter-Enlightenment' in Nuclear Policies , May, 2007, pp. 469-482.

assuring the security of these materials. Terrorist targets during civilian nuclear transport could include:

- Shipments of LEU from enrichment plants to fuel fabrication plants (the LEU might be seized for a radiological weapon);
- Shipments of LEU or mixed-oxide (MOX) fuel from fuel fabrication plants to reactor sites; and
- Shipments of plutonium from reprocessing plants to storage sites and fuel fabrication plants.

Terrorist organizations have selected nuclear power plants as potential targets for organized terrorist attacks. Since the possibility of the utilization of modern technologies by the terrorist organizations has been long foreseen and led to development control and security protection measures by a series of physical barriers and a trained security personnel, allowing nuclear plant operators to be ready to defend against such attacks, though terrorist organizations can separate or coordinate an air attack with aircraft or an unmanned air, and possibly penetrate the containment building of a nuclear plant.

3. Nuclear Renaissance Phenomenon and Proliferation Risk

Energy is an essential factor for economic growth, and as the developing world continues its demand for energy, the need is estimated to grow significantly. At the same time, the carbon-intensive energy sources the world now relies on - chiefly coal, petroleum, and natural gas - pose a grave threat as the growing concentrations of carbon dioxide in the atmosphere bring about climate change and ocean acidification. Nuclear energy is a major energy source today, with significant benefits (clean electricity, medical diagnosis and treatment, industrial and agricultural uses) and poses special risks (environment, health and safety, proliferation). At least three types of peaceful uses were foreseen for nuclear energy in the 1950s: electricity production; propulsion; and civil engineering and mining. Nuclear power was seen as the leading technology in the expansion of electricity production. For a time it was believed that this would not pose a weapons proliferation risk as plutonium created in the efficient operation of power reactors was thought to be incapable of being used for explosive purposes. Today and in near future, international community lives in a new time of drastic changes occurring in the world of nuclear energy, a period pinned by some as 'nuclear renaissance'. This transformation challenge brings benefits and risks together. Thus, we wish to underline the current picture, pointing out the main parameters for next generations. First, international system should find a reasonable balance to solve the ongoing sustainable development issues., as the human population is increasing and parallel to this reality energy and water demand is rising for human life quality. Also keeping the fact that problems such as global warming and industrial development causes energy prices increase in relation to cost-effect, both sides must be given adequate alternative energy supplies, as requirements energy prices cost effect

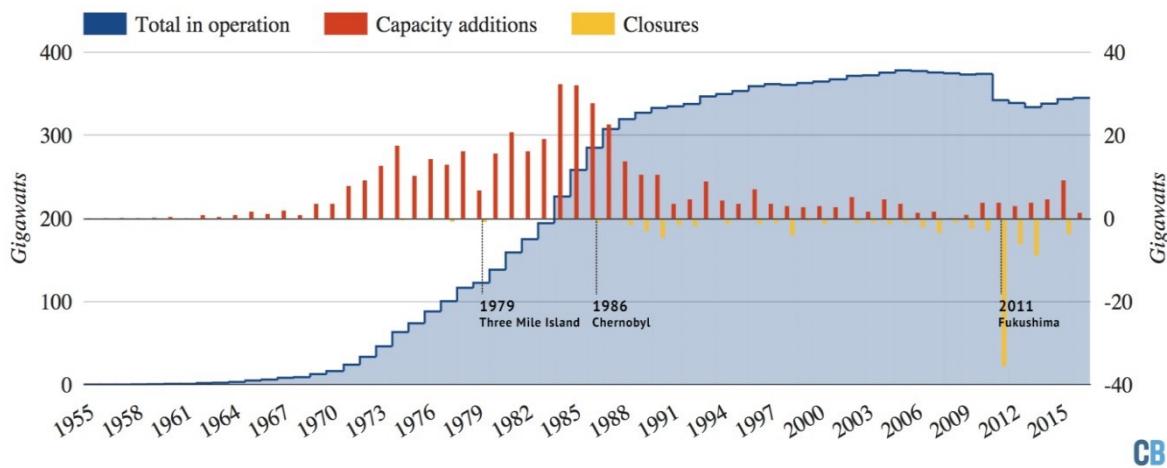
considerations. These bring a big necessity for supply and demand security in energy production for human civilization. In this regard, nuclear energy will be an alternative for the future generations.

- But most importantly, how can the security of nuclear energy and the elimination of the threat of proliferation of nuclear weapons threat be provided?
- Will the growth in global nuclear energy lead to the elimination of dangers including terrorism and increased risks, as mentioned above?
- How can we find common solutions to new kinds of problems?
- How should international organizations, institutions, and states give a new emphasis to problems that were regarded as lesser problems in the past, such as nuclear terrorism and the problem of illicit nuclear supply?
- What specific challenges to international security are created by the anticipated expansion and spread of civilian nuclear power?

Five serious, interrelated problems appear on the horizon: safety, sabotage, terrorist theft or purchase of a weapon or nuclear materials, nuclear weapons proliferation, and destruction of nuclear facilities in a conventional war. We need to create safer reactor technology for both national and international institutions. Fortunately, some measures, such as strong containment vessels and effective personal reliability programs, protect against both accidents and sabotages.

This risk can be limited if the acquisition of uranium enrichment or plutonium reprocessing technologies is discouraged or prohibited. These technologies are, however, also indispensable for the production of fuel for nuclear reactors. In the 25 years after the disaster of Chernobyl, nuclear construction declined while global demand for electricity more than doubled. As a result, nuclear's share of total electricity supplies peaked just shy of 18% in 1996 before falling to 11% in 2014. Today, more than 30 states have 450 reactors providing over 11% of the world's electricity supply (Figure-1).

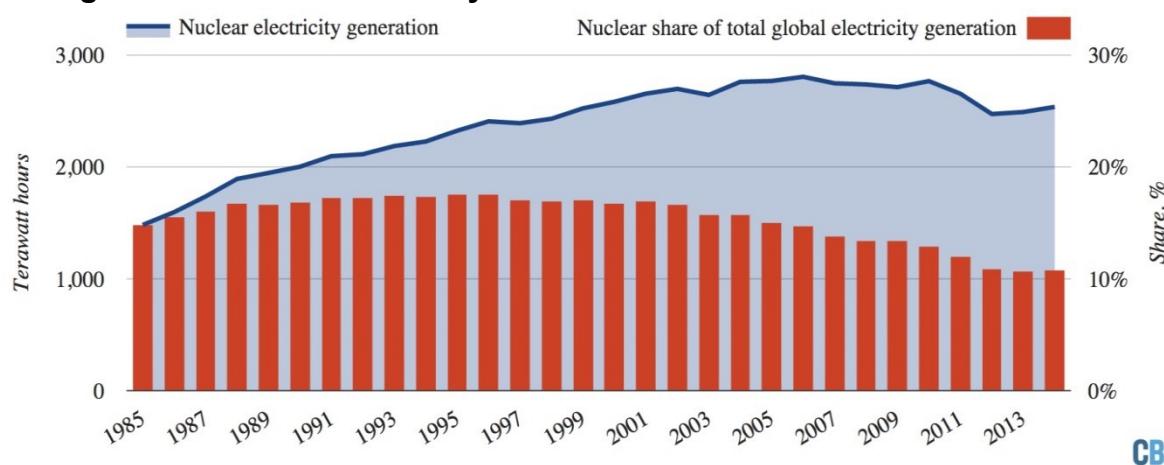
Figure-1: Global Nuclear Power Generating Capacity



Source: International Atomic Energy Agency (IAEA) [PRIS database](#) and Carbon Brief analysis. Chart by Carbon Brief.

IEA estimates that, states aim to use advanced technologies that will have the nuclear capacity reach to 1200 GW in 2050 representing 24% of electricity generated in global dimension (Figure-2). ⁵⁵

Figure -2: Nuclear Electricity Generation



Source: [BP Statistical Review of World Energy 2015](#) and Carbon Brief analysis. Chart by Carbon Brief.

States have also put serious effort into strengthening the legal framework of nuclear safety and security under the non-proliferation regime, which is suffering under the climate protection policies and competition from less costly renewable power. But the most interesting aspect of the renaissance is the large number of countries that do not

⁵⁵ "Mapped: The world's nuclear power plants", 8 March 2016, <https://www.carbonbrief.org/mapped-the-worlds-nuclear-power-plants>, (Accessed on 2 September 2017).

currently have a nuclear power plant yet have expressed an interest in building one. Waste management is a challenge that must also be confronted. Spent fuel needs to be handled in an appropriate way so as to protect current and future generations from the long-present threats including those created by reactor operations. Adequate security must be achieved as well. More reactors in more places mean more target sets for terror.⁵⁶ The growth of nuclear power presents challenges. One, of course, is the concern that the spread of nuclear technology could enable more countries to pursue nuclear weapons. Reactors are not the principal concern in this regard; rather, expansion of nuclear power might result in new countries undertaking fuel-cycle activities is the possibility that presents proliferation threats. The need for an assured fuel supply could cause more countries to develop their own uranium enrichment capacity.⁵⁷ The theoretical approach on the subject argues that civil nuclear cooperation does not lead to proliferation. Most scholars claim that nuclear weapons spread when states have a demand for nuclear bombs - not when they have the technical capacity for proliferation. Nuclear suppliers, for instance, generally restrict the sale of uranium enrichment or plutonium re-processing facilities because these can be used directly to produce fissile material for a bomb, but suppliers routinely build research or power reactors in other countries and train foreign scientists.⁵⁸

- What is the relationship between nuclear proliferation risk and nuclear plants' security?
- Will nuclear energy bring solution to the global warming problem, as an alternative to fossil fuels?

In this context, reactors themselves are not the problem. The problem is that, as more countries need nuclear fuel, there will be an inevitable demand for enrichment services. This means that the technology for enrichment could become even more widespread. The same technology used to produce low-enriched fuel for nuclear reactors can be used to produce highly enriched uranium, a weapons-usable material. There also is the possibility that some of these countries may proceed with reprocessing, raising the possibility that, if they were use today's reprocessing technology, they will produce separated streams of plutonium. Plutonium, of course, is also a weapons- usable material.

Russian Ministry of Foreign Affairs noted "the peaceful atom" is playing an ever-increasing role in satisfying the energy demand of the global economy. Existing and future nuclear power plants are instrumental to the economic growth, raising living

56 Richard A. Meserve, Robert Rosner, Scott D. Sagan and Steven E. Miller, "The Nuclear Future", *Bulletin of the American Academy of Arts and Sciences*, Vol. 62, No. 2, Winter 2009, pp. 71-76.

57 Richard A. Meserve, "The Global Nuclear Safety Regime", *Daedalus*, Vol. 138, No. 4, *On the Global Nuclear Future*, Vol. 1 , Fall, 2009, pp. 100- 111.

58 Matthew Fuhrmann, "Spreading Temptation: Proliferation and Peaceful Nuclear Cooperation Agreements", *International Security*, Vol. 34, No. 1, Summer 2009, pp. 7-41.

standards of the millions of people".⁵⁹ Another option, as President Obama himself put forward in his 2009 Prague speech is the establishment of a nuclear fuel bank, allowing countries to access peaceful power "without increasing the risk of proliferation". Even more fundamentally, many states today have been expressing an increasing interest in developing nuclear energy plants as a reliable resource ensuring their energy security. As the norms of international law have it, every sovereign state may establish its own facilities to enrich uranium, produce fuel and further possesses reprocessing rights.

It is important to have a discussion with the people we seek to influence, at a very early stage. The Academy has the unique capability to convene people across a broad spectrum of disciplines and from all over the world, to get all of the stakeholders to approach these problems together, and to try to find a path to a safer world. We need to revive the discipline of nuclear engineering, both for designing and building new plants and for operating them safely and efficiently, keeping to the stringent quality demands for construction of new nuclear plants as well as the supporting infrastructures.

4. The Role of International Law on Effective and Sustainable Mechanism for the Establishment of Global Nuclear Security Regime

Since above mentioned nuclear security and radiological protection measures necessarily involve key national functions such as law enforcement and control over the access to information, states are "understandably reluctant to expose their sovereign security and law enforcement practices to external scrutiny, let alone anything resembling external regulation".⁶⁰ I think the focal point on the issue of nuclear security is the states' obligation to obeying the role of international regulations regarding nuclear security law and why such rules are instrumental? Fundamentally, the International law aims to control the spread of nuclear weapons and eliminate illegal usage of illicit material, either fissionable or radiological, for terrorist violence. More importantly, these agreements promote and enforce international peace and stability under the UN Charter for human civilization.

There are a number of multilateral efforts aimed at assisting states in upgrading their physical protection systems. The first and most important one, NPT, was designed to prevent the states from diverging their use of nuclear materials from peaceful means to military purposes, that did not possess nuclear weapons as of 1967 and agreed not to obtain them in the future, but it has no provisions for dealing with physical protection standards, supporting states; but it has no provisions for dealing with physical protection standards. This non-nuclear weapon norm is given legal basis through the

59 Statement by the Deputy Minister of Foreign Affairs of the Russian Federation, Sergey A. Ryabkov at the 2010 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, May 4, 2010.

60 IAEA, 2003: 145.

Treaty on the Non-Proliferation of Nuclear Weapons (NPT), which was concluded in 1968 and came into force in 1970.⁶¹

I think that the role of international law in effective and sustainable mechanism for the establishment of a global nuclear security regime is crucial. One critical question is, is there currently a sufficient legal framework to provide an effective response against new challenges such as North Korean nuclear program to alleviate regional and global security concerns?

Nuclear relationships resulted by the collapse of the ideological divide in West-East relations, and the dissolution of the former Soviet Union resulted in the transformation of world affairs, and the radical differences of the sides involved in international order put nuclear proliferation concerns and non-proliferation strategies at the core of international security policies. States also accept through their possession that they agree to the responsibility of divesting themselves of these weapons over time. Also a significant multilayer legally binding treaty was signed in relevance to the physical protection of nuclear material in 1980 and 2005 amendment. In 2016 Nuclear Summit, 93 states have ratified the 2005 Amendment for physical protection convention, forming an important step for the implementation of nuclear terrorism and illicit trafficking. Many countries have taken further steps to strengthen the compliance with the NPT regime heralded with the disarming of Iraq 1991 by the UN Security Council and the penalties imposed upon it by the IAEA. In this regard, the IAEA has legally adopted the implementation of a new concept of nuclear transparency safeguard, in which much greater importance on the monitoring of nuclear activities, including imports and exports. The IAEA agency therefore has the right to request any additional information it requires to verify all the inventories of materials and equipment reported by the states.⁶² One of the most important steps taken was amending the 1980 Convention on the Physical Protection of Nuclear Material to encompass nuclear material within national borders as well as in international transit. In addition, in April 2004, the UN Security Council adopted Resolution 1540, while in 2005 an International Convention for the Suppression of Acts of Nuclear Terrorism was adopted by the UN General Assembly. Both of these oblige all states to take national measures to prevent terrorists acquiring nuclear material and technology for weapons purposes. The IAEA has also seized the initiative in making nuclear security one of its priority tasks. Another point to consider is that the end of the Cold War has opened the way to both greater international collaboration to prevent nuclear proliferation and led to a merger of nuclear arms control and non-proliferation activities. It has opened the prospect of a greatly enlarged role for the IAEA, not only in terms of the existing regime but also in two other areas. One is in safeguarding fissile materials recovered from dismantled

61 This treaty makes mandatory the 'acceptance of a monitoring and verification system over the nuclear activities of non-nuclear weapon states operated by the International Atomic Energy Agency (IAEA); sets out some constraints on their nuclear trading activities; and commits all parties to negotiate effective disarmament measures, particularly nuclear ones. It thus serves as the main foundation for the global nuclear non-proliferation regime.

62 IAEA News briefs, 7: I, January/February 1992; IAEA Press Release.

nuclear warheads, and the other is in providing secretariat, verification and inspection services for state parties to a CTBT.⁶³

Convention on the Physical Protection of Nuclear Material - CPPNM

The CPPNM was adopted on 26 October 1979, entering into force on 8 February 1987. It is one of thirteen counter-terrorism instruments developed by the international community, and is the only internationally legally binding undertaking for the physical protection of nuclear material. Its objectives include a worldwide commitment to:

- Achieving and maintaining effective physical protection of nuclear materials and facilities in the civilian nuclear fuel cycle;
- Preventing and combating offences relating to such material and facilities; and
- Facilitating appropriate co-operation among States Parties.

The Convention covers only nuclear material used for peaceful purposes during international transport and, with certain exceptions, in domestic use, storage and transport. It provides a categorization of nuclear material requiring appropriate levels of physical protection during storage and international transport. With the Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM/A) entering into force, the risks of nuclear terrorism and smuggling and illicit trafficking in nuclear materials are likely to be reduced. This agreement is a concrete success of the Nuclear Security Summit (NSS) process that was launched in Washington in 2010 and concluded with the summit in Washington on March 31, 2016.

Why is this so remarkable? There are some critical advantages for states signed into NPT membership status. It's a well-known reality that NPT member states have the opportunity of using nuclear technology for peaceful purposes "without discrimination" from nuclear supplier states. This is an important point of interpretation of the right to peaceful use in article IV, recognizing that every NPT party has the essential freedom to determine how it wishes to exercise this right. Other domain such as NPT membership does not guarantee a state access to civilian nuclear assistance and there are cases where this bargain goes unfulfilled. Indeed, recent research finds that, on average, NPT members are no more likely than non-members to receive sensitive nuclear assistance or sign peaceful nuclear cooperation.⁶⁴

Secondly, we need to establish global consensus for a functioning transparency system. In order to achieve this insurance factor; an already functional organization such as IAEA may contribute to realize transparency on the peaceful usage of nuclear powder around the globe. Regarding rising energy demand and global energy security picture, the degree to which the future nuclear order promotes safe, secure,

63 John Simpson, "Nuclear Non-Proliferation in the Post-Cold War Era", *International Affairs*, Vol. 70, No. 1, January, 1994, pp. 17-39.

64 Matthew Fuhrmann and Jeffrey D. Berejikian, "Disaggregating Noncompliance: Abstention versus Predation in the Nuclear Nonproliferation Treaty", *The Journal of Conflict Resolution*, Vol. 56, No. 3, June 2012, pp. 355-381.

proliferation-resistant, and effectively monitored and governed nuclear energy power will be a vital factor for next generations of human being.

However, there are still problematic policy positions maintaining legal interpretations of NPT article IV and article III. For example, in her opening statement to the 2010 NPT Review Conference, US Secretary of State Hillary Clinton stated: "*Potential violators must know that they will pay a high price if they break the rules, and that is certainly not the case today. The international community's record of enforcing compliance in recent years is unacceptable. So we need to consider automatic penalties for the violation of safeguards agreements such as suspending all international nuclear cooperation or IAEA technical cooperation projects until compliance has been restored.*"⁶⁵

Explained above is how the nuclear arms race has been evolving since the incidents of Hiroshima and Nagasaki, and the expansion in the number, power and sophistication of nuclear weapons. Nuclear Non-Proliferation Treaty-NPT is the international legal backbone of the global efforts to prevent the spread of nuclear weapons. The high contracting parties are under the legal responsibility to work for the elimination of radiological arms. NPT is meant to prevent nuclear proliferation while promoting the spread of nuclear technology. Article III of the NPT calls for safeguards, inspections, and transparency. Though the ratification of the NPT, States commit to forgo nuclear weapons and accept International Atomic Energy Agency (IAEA) safeguards designed to detect noncompliance. It is puzzling, therefore, that states would choose to be a part of the NPT while they were attempting to develop nuclear bombs. There is a symbiotic connection between peaceful nuclear cooperation and NPT membership. In its treatment of NPT article IV peaceful uses of nuclear energy, however, UNSC Resolution 1887⁶⁶ again displays essential continuity of the policies. The restrictions and conditions on nuclear supply which the Security Council here encourages States to adopt would appear to be based upon interpretations of both article III and article IV of the NPT. The nuclear order's legitimacy has therefore rested upon mutual obligation and reciprocity. NPT has functioned well in slowing down the process of proliferation.

To sum up, it is possible to say that the NPT has functioned well in slowing down the process of proliferation, through introducing some means of deterrence even as some

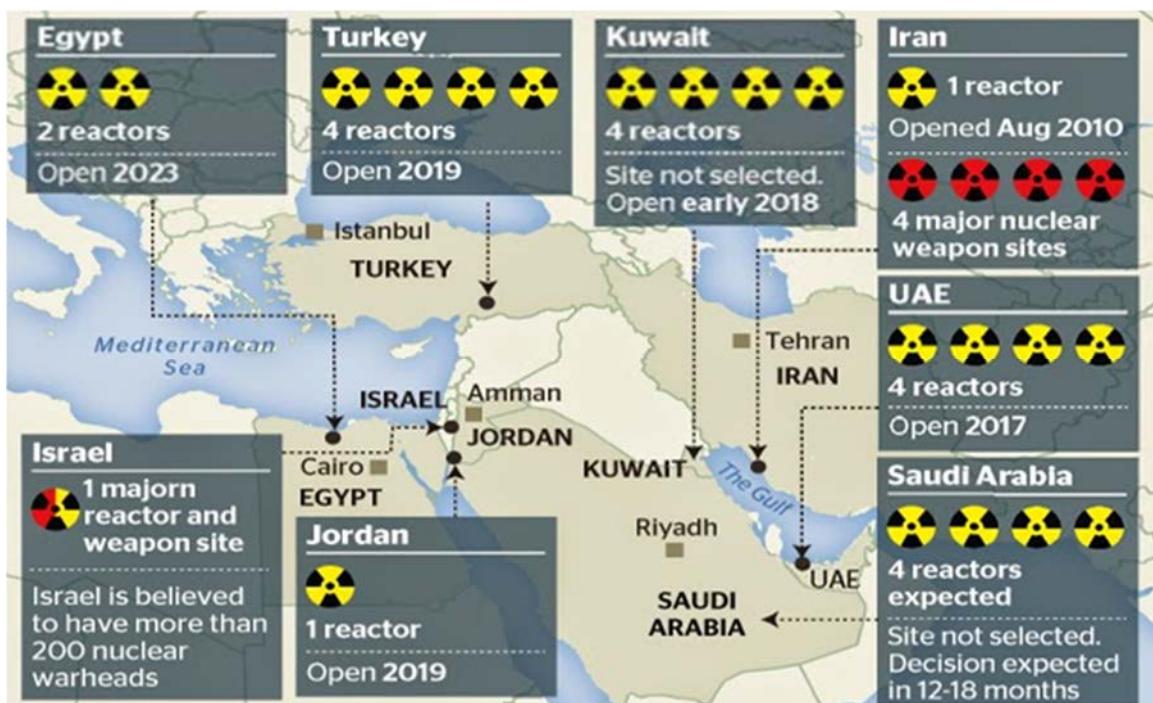
65 See, Daniel H Joyner, "Recent Developments in International Law Regarding Nuclear Weapons", *The International and Comparative Law Quarterly*, Vol. 60, No. 1, January 2011, pp. 209-224.

66 Resolution 1887: Encourages States to require as a condition of nuclear exports that the recipient State agree that, in the event that it should terminate, withdraw from, or be found by the IAEA Board of Governors to be in non-compliance with its IAEA safeguards agreement, the supplier state would have a right to require the return of nuclear material and equipment provided prior to such termination, non-compliance or withdrawal, as well as any special nuclear material produced through the use of such material or equipment; [and] Encourages States to consider whether a recipient State has signed and ratified an additional protocol based on the model additional protocol in making nuclear export decisions;

leaders seek to pursue the benefits they perceive to rise from the possession of nuclear weapons. New approaches will be required to build up a norm against nuclear possession and transform the current, divided non-proliferation regime into a global security framework, codified through some form of universally applicable nuclear weapons convention.⁶⁷

5. The Case of Turkey and the Establishment of Nuclear Security

After reviewing the global case, it should be reminded that with its rapidly growing energy demand, Turkey will complete new NPP's in Mersin and Sinop soon. While government attaches a great importance to country's energy strategy, physical security of nuclear materials has emerged as a highly crucial topic for national and international security. As President Erdoğan states in 2016's Nuclear Security Summit, "Turkey has taken an active part in the Nuclear Security Summit process since its inception". Firstly, it could be argued that to have effective, sustainable solution to defend against new physical nuclear threats, we need to achieve worldwide cooperation, build confidence dialogues that would have all states working together for risk management, making decision makers much more aware under international law responsibilities. Thus, this paper's aim is to academically search the ways of improving nuclear materials security culture globally and discuss a road map for Turkey by comparing the best practices of nuclear material protection in worldwide and by benefiting from IAEA's deep capabilities.

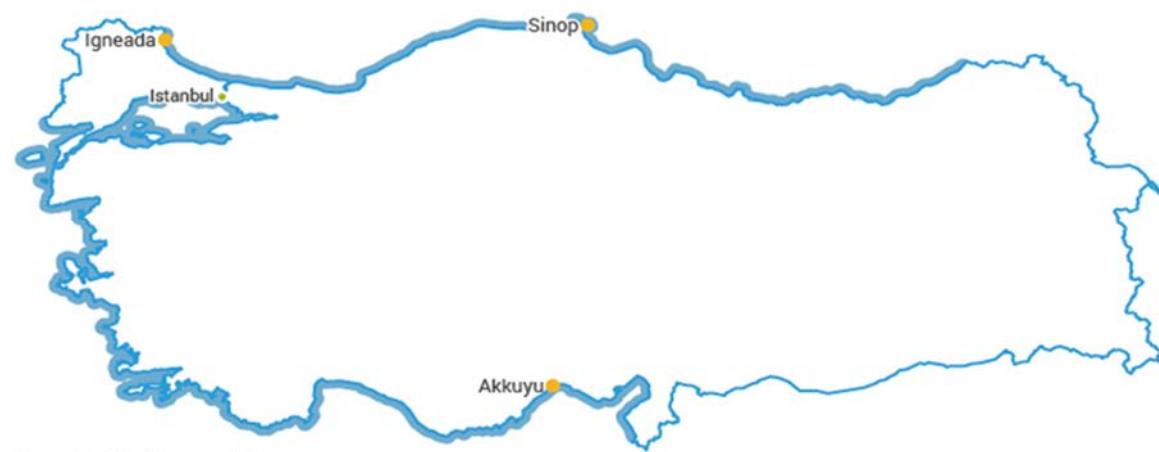


⁶⁷ Rebecca Johnson, "Rethinking the NPT's Role in Security: 2010 and Beyond", *International Affairs*, Vol. 86, No. 2, March 2010, pp. 429-445.

Source:

http://1.bp.blogspot.com/-nniXrHoNPD0/VDi_5mro97I/AAAAAAABQFg/oSmGk9G4Yug/s1600/Nuclear__2__65999a.jpg.

Planned Nuclear Power Plants in Turkey



Source: World Nuclear Association

Source:

<http://www.world-nuclear.org/getmedia/c4882a7d-25b1-46cc-aade-cc6dc01e315b/planned-nuclear-power-plants-in-turkey.png.aspx>.

In Turkish case, it is necessary to point out some significant parameters of Akkuyu and Sinop Nuclear Power Plant deals. In both of these deals, the main obligation of Turkish side is to provide the land and the necessary infrastructure that the nuclear power plant will be constructed over without demanding cost. And also the Turkish side guarantees to purchase the generated electricity for a determined period of time through TEİAŞ (Türkiye Elektrik İletim A.Ş.). This period has been determined as 15 years for Akkuyu and 20 years for Sinop. Moreover, in both of these agreements, Ankara is obliged to provide every kind of facilitations on permission, licensing and authorizations as long as its laws allow. The chief obligation of Russia on Akkuyu's construction is to set up a company with hundred-percent Russian capital according to Turkish laws.⁶⁸ This company is currently operational as Akkuyu Nükleer A.Ş. Russia will operate the four-unit nuclear power plant after completing it within the 10 years after obtaining all necessary permits. After that it will provide electricity to Turkish side while it is

68 Azime Telli, "Türkiye'nin Nükleer Enerji Açılımının İçerik Analizi: Çeşitlendirme mi, Teslimiyet mi? / Content Analysis of Turkey's Nuclear Energy Initiative: Diversification or Submission?", *Bilge Strateji*, Cilt: 8, Sayı: 14, Bahar 2016, p. 65.

functional. Furthermore, the nuclear wastes will be under the responsibility of Moscow and will be transferred to Russian Federation.

Regarding Sinop, a Japanese firm will construct the four-unit plant and after becoming operational, it will operate the power plant through generating electricity during its time of service. In this agreement, the responsibility of nuclear wastes has been given to the Turkish side. In both of these agreements, the costs of nuclear power plants subtracting from the management have been granted under the responsibilities of project companies. In addition to this, the nuclear reactor type in Sinop has been determined as ATMEA1. On the other hand, there exists no clause in Akkuyu agreement on the type of nuclear reactor as VVER 1200. When the conditional-dependent time frames instead of dates on the completion periods of units are the case, in Sinop, the dates that the units will become operational have been clearly specified. In Akkuyu, the construction works have yet begun due to licensing process of TAEK.

 **Akkuyu Nuclear Power Plant is the First Rosatom BOO Construction Project Outside Russia** 

Akkuyu Project Features

- First Nuclear Power Plant in Turkey
- First Rosatom BOO (build-own-operate) project. Under the IGA, Rosatom is responsible for engineering, construction, operation and maintenance of the plant.
- Legal basis: Intergovernmental Agreement, May 12, 2010
- Project design: AES-2006 (VVER-1200)
- Total capacity: 4,800 MW. (4 x 1200 MW)
- Implementation period: 2011-2023
- Total cost ~ \$ 20 bln
- Power Purchase Agreement for 15 years, fixed price terms
- Support of the Russian and Turkish Governments
- Maximization of Turkish personnel involvement in construction and operation of the plant.
- Job creation potential – up to 10 000 for the construction only

Akkuyu site, Turkey

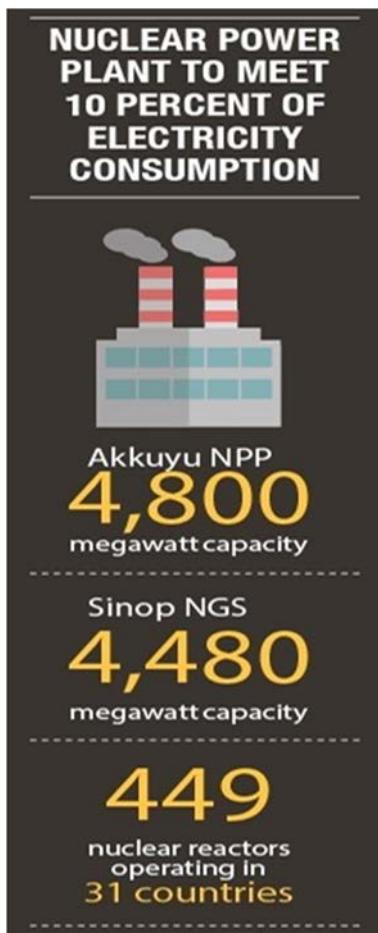


| 5

Source:

<http://slideplayer.com/slide/4782528/15/images/5/Akkuyu+Project+Features.jpg>.

When the waste management case is considered, the waste management and waste abolishment will be under Moscow's responsibility in Akkuyu Nuclear Power Plant Agreement. The wastes will be transferred to Russia and if Turkey wants them, it will have to pay in return for a cost. Moreover, in case of reaching an agreement between parties, there is a clause on the re-processing of the used Russian nuclear fuel by Moscow. The used fuel and radioactive waste management in Sinop has been granted under the responsibility of Turkish government. The project company will be responsible for the management of the wastes until they transport into the final



abolishment facility under the government's responsibility. The project company will provide the necessary money to the funds in order to meet all the expenses of waste management in parallel with Turkish laws.⁶⁹ When we come to fuel supply, this issue has been included among the fields that the both sides will cooperate on Aim and Content part. The fuel supply and fabrication subjects are totally under the control of Project Company which means that it has been granted totally under the control by Russian Federation. As the operator of nuclear power plant, the fuel will be supplied by Moscow. It should not be forgotten that Russia has an important share in nuclear fuel market. Moreover, the technology used in Akkuyu Nuclear Power Plant is just suitable for the use of Russian fuel. This means a dependence on Russia regarding the nuclear fuel. The agreement also includes the establishment and operation of a nuclear fuel production facility in Turkey by the Russian Federation. But the establishment of this facility and nuclear fuel cycle will be determined by the consensus of both parties and the details on facilities and method have not been included in the context of agreement. The Sinop agreement has granted the fuel supply to the project company. The purchasing of fuel to be used in nuclear power plant and the making of supply agreement are under the responsibility of a project company.

France is one of the important nuclear fuel supplier countries which take place in the list of OECD's nuclear report. In this project, it is expected the use of fuel acquired from France and there is no special clause on this issue. Within the context of the agreement, the responsibility of setting up a nuclear fuel production factory on the area granted by the government will be under the responsibility of EÜAŞ on behalf of Turkish side. The project company's obligation has been determined as to the provision of contacts between project's contractor company and parties as well as to show the maximum efforts regarding the collaboration with the Japanese government.⁷⁰

Source:

<https://iadsb.tmgrup.com.tr/94326c/0/0/0/220/761?u=https://idsb.tmgrup.com.tr/2017/08/10/turkey-to-expand-capacity-to-meet-energy-needs-with-3-nuclear-power-plants-in-action-1502395396261.jpg>.

69 Telli, "Türkiye'nin Nükleer Enerji Açılımının İçerik Analizi: Çeşitlendirme mi, Teslimiyet mi? / Content Analysis of Turkey's Nuclear Energy Initiative: Diversification or Submission?", p. 67.

70 Telli, "Türkiye'nin Nükleer Enerji Açılımının İçerik Analizi: Çeşitlendirme mi, Teslimiyet mi? / Content Analysis of Turkey's Nuclear Energy Initiative: Diversification or Submission?", p. 68.

Regarding the operational status of Akkuyu Nuclear Power Plant, which is to be constructed in Mersin; Berat Albayrak, the Minister of Energy and Natural Resources of Turkey, has underlined that “*the plant will be operational by 2023. We plan to take Akkuyu into service in 2023. The plant will have the highest of international security standards and will use 3+ technology*”.⁷¹

The European Parliament's (EP) latest resolution on suspending accession talks surprisingly did include a paragraph calling on the Turkish government to stop the construction of the Akkuyu Nuclear Power Plant (NPP). EP's resolution regarding Turkey on 6 July 2017 would mention “*Calls on the Turkish government to halt its plans for the construction of the Akkuyu nuclear power plant point out that the envisaged site is located in a region prone to severe earthquakes, hence posing a major threat not only to Turkey, but also to the Mediterranean region. The Turkish government should consult Greece and Greek Cypriot governments about further developments at the Akkuyu NPP due to environmental concerns.*”⁷² But for some energy experts, these demands and allegations are regarded as unrealistic and these are targeted at damaging Ankara's energy supply security. For instance, Dr. Sohbet Karbuz from the Mediterranean Observatory for Energy (OME), an energy industry association in Paris, has stated that “*the EP's call about Akkuyu NPP as absurd and politically motivated, if not malicious.*” On the other hand, Aleksandr Uvarov, the chief editor of the AtomInfo, has highlighted that “*the EP's call is not related to earthquake hazards. The EP's call about Akkuyu is line with EU's political and economic interests and it has nothing to do with earthquake hazards*”. Sergey Kirienko, Rosatom's former director general would state in 2015 that “*the construction of Akkuyu was designed to withstand up to 9 magnitudes on the Richter scale. Akkuyu is "not in an earthquake zone" and that the new plant will in any case be built to withstand earthquakes up to a magnitude of nine on the Richter scale. Modern reactor technology would have averted the Fukushima-Daiichi accident that occurred in Japan in 2011*”. Professor Erdal Tanas Karagöl from the Energy Research Department at the Ankara-centered Political, Economic and Social Research Foundation (SETA) think tank has underlined that “*EP's call targets Turkey's energy supply security, and is unacceptable. Turkey has been diversifying its energy supply sources with the aim of meet increasing energy demands for its growing economy. Thus nuclear power is essential for Turkey and the Akkuyu NPP project is a big step to strengthen Turkey's energy supply security. The environmental impact assessment report of the Akkuyu NPP has already evaluated the earthquake*

71 “Turkey's first nuclear power plant Akkuyu to be operational by 2023”, *Daily Sabah Energy*, 3 February 2017, available at:
<https://www.dailysabah.com/energy/2017/02/04/turkeys-first-nuclear-power-plant-akkuyu-to-be-operational-by-2023>, (Accessed on 23 August 2017).

72 Ali Ünal, “EP call on Turkey to halt Akkuyu Nuclear Power Plant ‘not related to hazards’”, *Daily Sabah Energy*, 7 July 2017, available at:
<https://www.dailysabah.com/energy/2017/07/08/ep-call-on-turkey-to-halt-akkuyu-nuclear-power-plant-not-related-to-hazards>, (Accessed on 23 August 2017).

risk and it has approved the construction of the NPP project. Therefore I believe that the EP's call only aims to weaken Turkey's energy supply security rather than stressing earthquake risk".⁷³



Source:

<http://www.thecypriotpuzzle.org/wp-content/uploads/2015/03/CAYxah6UMAABVqu.jpglarge.jpg>

Of course, same as all peaceful nuclear energy actors, Turkey needs international cooperation with international community and IAEA at national level, increasing highly sensitive attention is being paid to "guns, guards and gates" as the primary means of achieving security at all types of nuclear installations.

Within the context of Turkey's first nuclear power plant⁷⁴, an important event would occur on April 3, 2018 with the realization of ground-breaking ceremony of Akkuyu Nuclear Power Plant (Akkuyu NPP) by the participation high level officials from Turkey and the Russian Federation via teleconferencing system to the ceremony in Akkuyu, Mersin. In this ceremony, Recep Tayyip Erdoğan has shared the following statements on this project;

"Turkey aims to be among the top 10 economies of the globe and that it will thus have bigger need for energy. We uninterruptedly continue with our investments in every branch of the energy industry in line with our objective of boosting our energy security. Nuclear energy holds an important place in our plans for a

⁷³ <https://www.dailysabah.com/energy/2017/07/08/ep-call-on-turkey-to-halt-akkuyu-nuclear-power-plant-not-related-to-hazards>.

⁷⁴ For more information on this issue please see, Mesut Hakkı Caşın and Sina Kısacık, *Avrupa Birliği Enerji Hukuku ve Güvenlik Algılamaları*, (İstanbul: Çağlayan Kitap & Yayıncılık & Eğitim, 2018), pp. 371-416, Ozan Örmeci and Sina Kısacık, *Rusya Siyaseti ve Rus Dış Politikası: Teorik Çerçeve-Tarihsel Arka Plan-Örnek Olaylar*, (Ankara: Seçkin Yayıncılık, Haziran 2018), pp. 451-469.

future in which our country will have sound and sustainable energy. Currently, 31 countries obtain a significant portion of their electricity from 450 active nuclear power plants all around the world. And there are 55 nuclear power plants under construction in 16 countries at present. This number will rise to 56 with the Akkuyu Nuclear Power Plant, for which we have broken ground. With the launch of the Akkuyu Nuclear Power Plant's first reactor in 2023, Turkey will have joined the group of countries using nuclear energy. We will thus have crowned the centennial of our Republic with a historic work in the field of energy. Akkuyu Nuclear Power Plant will supply 10% of Turkey's electricity demand after it becomes operational with all its units. Turkey's energy basket, which is still mainly based on oil, natural gas and coal, thus, will become healthier. They will continue to work together in line with their goal of launching the first of four reactors of the Akkuyu Nuclear Power Plant in 2023 and they are determined to continue and further strengthen their cooperation with Russia on regional issues, too".⁷⁵



Source: <https://www.energy-reporters.com/production/putin-and-erdogan-mark-joint-nuclear-project/>.

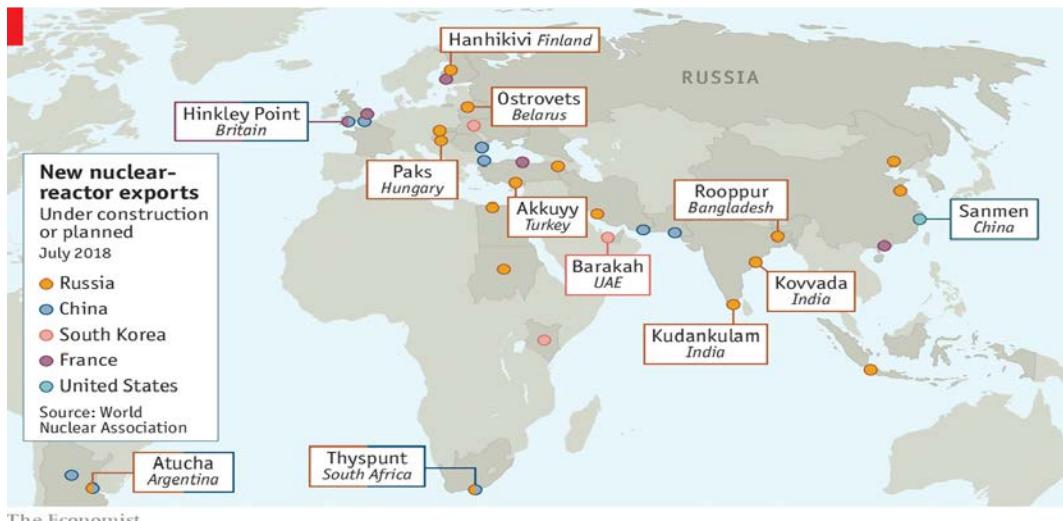
At the same ceremony, Vladimir Putin, the president of the Russian Federation, has stressed the significance of Akkuyu NPP as follows;

"First, I would like to sincerely congratulate all of you on the start of the construction of the first power unit of the Akkuyu Nuclear Power Plant. The significance of this great innovative project is hard to overestimate. In fact, today we are not simply present at the construction of the first Turkish nuclear power

⁷⁵ Presidency of the Republic of Turkey, "We are witnessing a historic moment in terms of energy cooperation between Turkey and Russia", 3 April 2018, available at: <https://www.tccb.gov.tr/en/news/542/92209-we-are-witnessing-a-historic-moment-in-terms-of-energy-cooperation-between-turkey-and-russia->, (Accessed on 18 September 2018).

plant, but we are witnessing the laying of the groundwork for Turkey's nuclear industry. We are creating a new industry. Turkey is a highly developed country in terms of technology and economics, but this is a new phase, a new step in the development of the Turkish economy. Russia is one of the recognised leaders in the peaceful use of nuclear energy. The Akkuyu project will involve the use of the most advanced engineering techniques, the most cost-effective and reliable technologies – the technologies we use for our own projects in Russia. The highest safety standards and the most stringent environmental requirements will also be observed. The opening of the plant will serve the development of the Turkish economy, its research and production potential, and will provide Turkish consumers with inexpensive and 'clean' electricity. According to expert estimates, this nuclear power plant will account for about 10 percent of Turkey's overall power generation, as was already mentioned. I would like to note that Russian contractors are planning to attract Turkish small and medium-sized businesses to the project; they intend to contract a significant part of the resources for the future station in Turkey. More than 350 Turkish companies have already applied for inclusion in the list of potential suppliers. The Akkuyu project will create new, modern and, very importantly, highly paid jobs in Russia and Turkey, as well as boost the development of advanced producers and technologies. We also intend to closely cooperate in training skilled personnel to operate the plant. As mentioned, over 220 Turkish young people are studying nuclear engineering at Russian universities. The 35 Turkish citizens who have graduated from one of the world's leading universities in this area, the National Research Nuclear University MEPhI, have received employment offers from Akkuyu Nuclear, the plant's project company. I am glad that some of them are attending this ground-breaking ceremony. We are grateful to our Turkish colleagues for designating this project a strategic investment project and for expanding the list of tax incentives and preferences. I would like to thank all our Turkish friends for this decision. It has made our project economically expedient and profitable. I would also like to thank members of the Turkish parliament. What you have done will make the project much more attractive to potential investors. Dear friends, we are facing the ambitious goal of launching the first power unit in 2023, the year of the 100th anniversary of the Republic of Turkey. My dear friend Recep Tayyip Erdogan and I have agreed that we will do our best to attain this goal. I am confident that our plans will be implemented thanks to close interaction between the Russian and Turkish professionals involved. The successful implementation of this project will become a symbol of the dynamic and consistent development of Russian-Turkish interaction, partnership and friendship. I wish success to all participants in this project. All the best.”⁷⁶

⁷⁶ President of Russia, “Akkuyu Nuclear Power Plant ground-breaking ceremony”, 3 April 2018, available at: <http://en.kremlin.ru/events/president/news/57190>, (Accessed on 18 September 2018).



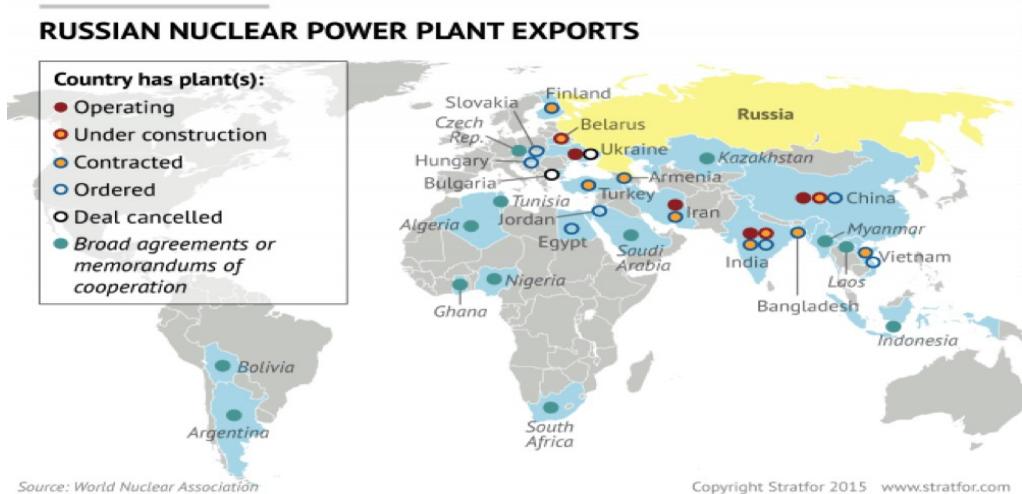
Source: [https://www.economist.com/europe/2018/08/02/the-world-relies-on-russia-to-build-its-nuclear-power-plants.](https://www.economist.com/europe/2018/08/02/the-world-relies-on-russia-to-build-its-nuclear-power-plants)

At the same ceremony, Berat Albayrak, the then Minister of Energy and Natural Resources of Republic of Turkey, has shared the following remarks regarding the significance of Akkuyu NPP⁷⁷:

"The 63 year-dream has realized. The intergovernmental between Turkey and Russia was signed in 2010. We are making ground-breaking of the greatest project of Turkey with the cost of 20 Billion U.S. Dollars. Akkuyu NPP will play a very important role in Turkey in terms of capacity and energy supply security. Thanks to this project, we will generate electricity uninterruptedly for 7 days and 24 hours without being dependent on climate and seasonal conditions. We will do with zero emissions in other words doing this without any zero greenhouse emissions damaging the environment. The nuclear energy will provide an important capacity to us ranging from industry, agriculture, satellite communication to health. When this nuclear technology capacity is considered, today in Turkey, we are experiencing a very significant turning point in energy and technology. We will generate latest technology energy which has the highest security standards with Akkuyu NPP. With the beginning of the construction, 10.000 people will be employed and eighty percent of it will be Turkish employees. Most of the goods and equipments needed during the construction and management will be supplied by Turkish firms. The joint investments with foreign countries and firms in nuclear energy will provide high level know-how as well as technology transfer both to our country and to this field. 35 of 248 students going for training to Russia have completed their

⁷⁷ Elisabeth Dyck, "Turkey Starts Construction of its First Nuclear Power Plant", *International Atomic Energy Agency (IAEA)*, 5 April 2018, available at: <https://www.iaea.org/newscenter/news/turkey-starts-construction-of-its-first-nuclear-power-plant>, (Accessed on 18 September 2018).

trainings and returned to Turkey in previous months. I believe that our students' knowledge and experiences will play very important role in the nationalization of nuclear technology. The decisiveness shown by the leaders of two countries is very significant for the project's coming in to the phase of realization. The Akkuyu NPP will play a leading role for the collaborations between Turkey and Russia in other fields".⁷⁸



Source: <https://oilprice.com/Alternative-Energy/Nuclear-Power/Why-Nuclear-Energy-Is-Critical-For-Russia.html>.

The Greek Cypriot government spokesman Prodromos Prodromou has underscored that Nicosia will organize the required activities and protests against the construction and the being operational of Akkuyu NPP Project of Turkey. He has shared the following remarks on this issue;

"The decision for the construction and operation of this nuclear power plant on the southern coast of Turkey "raises concerns for a possible impact in terms of safety because such a power plant in this area affects our country much more than the largest part of the Turkish territory. Cyprus is more concerned than any other country since the power plant will be situated just a few dozen kilometres from its northern coast. Turkey did not take into account the grave reservations expressed by various quarters, nor did it heed the European Parliament's call to terminate the construction plans since this is a seismologically vulnerable area. Neither has it taken into consideration the call to adopt the Espoo Convention on the transborder environmental effects. Ankara ignored the fact that it was asked in last July's Progress Report on Turkey to "at least consult

⁷⁸ Türkiye Cumhuriyeti Enerji ve Tabii Kaynaklar Bakanlığı Nükleer Enerji Proje Uygulama Dairesi Başkanlığı, "Akkuyu Nükleer Güç Santrali Temel Atma Töreni - Enerji ve Tabii Kaynaklar Bakanı Berat Albayrak, Beştepe'deki Cumhurbaşkanlığı Külliyesi'nde düzenlenen Akkuyu NGS'nin temel atma töreninde konuştu.", 3 April 2018, available at: <https://nepud.enerji.gov.tr/tr-TR/Haberler/Akkuyu-Nukleer-Guc-Santrali-Temel-Atma-Toreni>, (Accessed on 18 September 2018).

with the governments of neighbouring countries, such as Greece and Cyprus. Through these actions, Turkey creates conditions of instability and possible dangers, and it seems to ignore obligations deriving from its relations with the EU, and the need for good neighbouring relations”⁷⁹

The partaking of the financial burden of the Akkuyu plant stays one of the most central points of the agreement settled in 2010. Half of the project would be sponsored by the Turks, which should return significant incomes for Russia in the long term, and upturn its geopolitical presence in this part of the world. Turkey or Turkish private sector companies stand to afford 49 percent of the investing in. Russia will be controlling supervision and management. For several years now, lots of Turkish technicians and personnel are being educated in Moscow. Russia stays searching long-term guarantees for the projects and similarly financiers who make the sponsoring problematic as Turkish company's displayed unwillingness to join in.⁸⁰ Two key Turkish firms Kalyon and Kolin have withdrawn from an offered deal to obtain 49 percent of the facility, sparkling for some time question marks on the future of the project. On the other hand, Rosatom has declared that in spite of the taking away of investors from the project, it is still devoted to progress and is supposing to obtain soon the construction license to begin building the plant. Rosatom has also underlined that it stood in negotiations with Turkish state-owned power producer EUAS in the aftermath of the breakdown of the contract with the two other large Turkish industrial holding firms nonetheless what stays definite present day that the selling of a 49 percent share in the plant has been put off from 2018 to 2019. The Chief Executive Officer of Rosatom, Alexei Likhachev has underscored that “*The probability to close the deal on the stake sale of the plant is low this year but it is likely to take place in the next year*”. Rosatom has acquired on Monday, just one day before of Putin's visit, a full construction license from Turkey's atomic energy authority, Xinhua has learned from informed sources who claim that the 2023 may still be in danger and that a new postponement stays conceivable. Kerim Has has highlighted that “*There are still many uncertainties in the future of the Akkuyu project. It is intertwined with politics and Russia wants Turkey to do its part in it, insisting that funding issues will eventually seal its faith*”.⁸¹ On the other hand Alexandre Novak, the Energy Minister of the Russian Federation has stressed the following issues with regard to the construction of Akkuyu NPP and Turkey's future plans to construct new nuclear power plants;

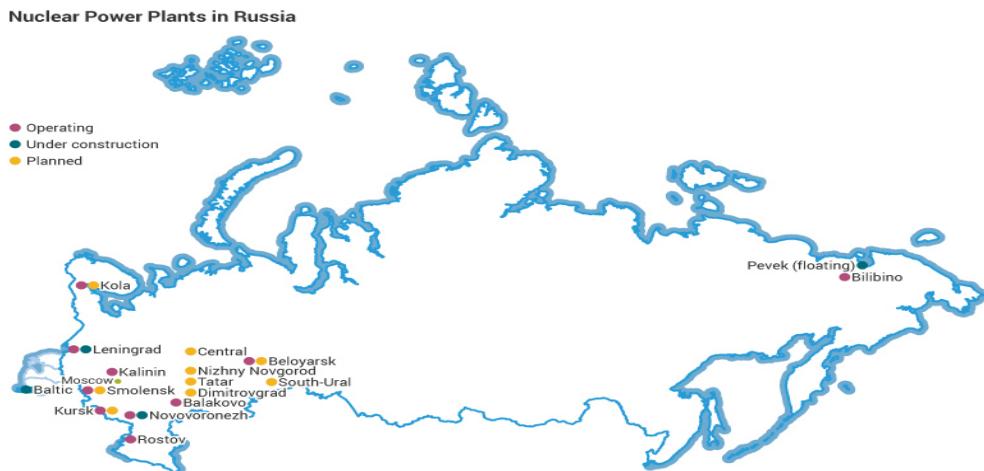
“Russia is able to complete the construction of Turkey's Akkuyu NPP even if it is unable to attract other investors. Already, \$3 billion has been invested and the figure is sufficient to complete the construction of Akkuyu. If investors will

⁷⁹ “Nicosia to protest construction of Akkuyu nuclear plant”, *Ekathimerini: News*, 5 April 2018, available at: <http://www.ekathimerini.com/227454/article/ekathimerini/news/nicosia-to-protest-construction-of-akkuyu-nuclear-plant>, (Accessed on 18 September 2018).

⁸⁰ “Spotlight: Turkey's first nuclear power plant project goes forth despite setbacks”, *Xinhua: New China*, 4 April 2018, available at: http://www.xinhuanet.com/english/2018-04/04/c_137086211.htm, (Accessed on 18 September 2018).

⁸¹ http://www.xinhuanet.com/english/2018-04/04/c_137086211.htm.

not be found for the 49 percent of the project, it means that the plant will be built by Rosatom. We prioritize Turkish companies in our negotiations, particularly firms in which state institutions have a stake. I hope that the agreement to include more investors will be finalized soon. Russia will notify of its intention to participate in more nuclear power plant projects if Turkey plans to extend nuclear power capacity with more plants".⁸²



Source: <http://www.world-nuclear.org/information-library/country-profiles/countries-overviews/russia-nuclear-power.aspx>.

Professor Mesut Hakkı Caşın has evaluated the significance of Akkuyu NPP with Turkey's decisiveness to purchase Russian S-400 Long Range Air Missile Defence System in terms of developing Ankara-Moscow relationships as follows;

"As you know, Turkey and Russia are implementing the Akkuyu nuclear power plant joint project. A nuclear power plant is a vital installation from a military-strategic point of view. In this regard, I believe that the S-400 systems will be effectively used to protect this nuclear power plant. Turkey has decided to purchase these units, keeping in mind these considerations. Turkey decided to purchase Russian-made S-400 systems along with Franco-Italian Eurosam SAMP-T defense systems. Turkey is not the only NATO country that uses Russian defense missile systems. Today Russian missile defense systems are being used by seven NATO member states, including the countries of the former Eastern Bloc and Greece. If Turkey urgently needs these [Patriot] missiles, the [Turkish] government will make an appropriate decision and these missiles will go into service in Turkey. On the other hand, the [Patriot] battery is currently being deployed on the territory of Turkey as part of the NATO system that provides air defense to Turkey. [However], if the US really wants to sell Turkey

⁸² "Russia willing to build more nuclear plants in Turkey", *Daily Sabah: Business / Energy*, 6 April 2018, available at: <https://www.dailysabah.com/energy/2018/04/07/russia-willing-to-build-more-nuclear-plants-in-turkey>, (Accessed on 18 September 2018).

these [Patriot] missiles, why, then, have the negotiations been going on for 10 years? Why has Washington hesitated to take this step earlier? Why have they raised the issue of selling the Patriot [surface-to-air missile system] after Turkey decided to buy the S-400?”⁸³

Within the context of Turkey's decision to have the nuclear power, apart from its intention to construct a second nuclear power plant in Sinop in the north of the country with Tokyo's involvement, along with Akkuyu, Turkish Minister of Energy and Natural Resources Fatih Dönmez has pointed out that building of the third nuclear power plant in Turkey, which is scheduled to be constructed in the Thrace region in the European part of the country⁸⁴, will be instigated in cooperation with China. Minister Dönmez has shared the following remarks on this issue:

*“We want to build the third nuclear power plant in Thrace; this work will be conducted with the Chinese specialists. The exact location has not yet been determined ... we have the highest electricity consumption in Istanbul and the Marmara region, so we consider Thrace as the best place for a nuclear power plant. After engineering studies, we will determine the right place for sure. China is one of the countries actively implementing the construction of nuclear power plants. In addition, they are quite open in the technology transfer. Therefore, we will build the third nuclear power plant with China”.*⁸⁵

Conclusion

If the U.S., South Korea, Japan, and China do not find some answer to North Korea's nuclear and missile programs, they are all going to have to respond by military means. The main risk is not the potential North Korean nuclear threat posed today. It is what can so easily come into being over the coming decade: An open-ended nuclear arms race in Northeast Asia with players whose actions and level of restraint in any given crisis is far harder to predict than the impact of mutual assured destruction in the Cold War. However, nuclear energy represents a dilemma in the possibility of its peaceful usage and the possibility to engage in the development of nuclear weapons,

⁸³ “Turkey to Use Russia’s S-400 Air Defense System to Protect Akkuyu NPP – Academic”, *Sputnik International: Opinion*, 28 March 2018, available at: <https://sputniknews.com/analysis/201803281062974799-turkey-russia-s400-akkuyu/>, (Accessed on 19 September 2018).

⁸⁴ “Turkey to Build Its 3rd Nuclear Power Plant on Bulgarian Border”, *Novinite: Sofia News Agency*, 6 April 2011, available at: <https://www.novinite.com/articles/127024/Turkey+to+Build+Its+3rd+Nuclear+Power+Plant+on+Bulgarian+Border>, (Accessed on 19 September 2018).

⁸⁵ “Turkey to build third nuclear power plant together with China”, *Trend News Agency*, 8 August 2018, available at: <https://en.trend.az/world/turkey/2938307.html>, (Accessed on 18 September 2018). Also please see, World Nuclear Association, “Nuclear Power in Turkey”, Updated June 2018, available at: <http://www.world-nuclear.org/information-library/country-profiles/countries-t-z/turkey.aspx>, (Accessed on 18 September 2018).

in our day. On one side, countries, such as Turkey, need to take advantage of nuclear energy using it to balance the energy demand of the growing market, on the other side, countries that are not a party or seceded from the partnership of NPT and those non-state actors trying to lay their hands on nuclear facilities still pose a possible threat to the international peace, security and stability. A delicate balance between these two opposite sides must be established in order to allow peaceful and secure usage of nuclear energy.

- How can we ensure the secure development of the nuclear energy market in the 21st century, while avoiding a possible crisis with North Korea and prevent the negative effects that would stem from such an incident?
- How will international community determine about states acquiring advanced nuclear security technology?
- How can the states' concerns resulting from the establishment of nuclear energy security and prevent terrorist threats are addressed?

These are the critical questions for creating a more secure future for the global nuclear energy market, the challenges that must be answered and met being also as crucial. Based on the focus of this brief paper, the world is at a crossroads in spite of the opposite views on the further spread of nuclear power on security groups' ideas, we should get ready to live with the reality that usage of nuclear energy in power plants will increase. In the next 40 years, we will see a growing number of states becoming active players in the NPT system. In this critical point the NPT regime will be the core of the solution for peaceful energy policy and preventing illegal nuclear activities. Establishment of this critical balance must maintain strong ties with NPT legal framework, nuclear energy spread and security will serve as a buffer factor between peaceful nuclear energy programs and possible development concerns of proliferation of nuclear weapons.

Of course, peaceful sustainable development and energy security are not very clear enough to predict confidence building whether the global nuclear renaissance phenomena future will be characterized by peace and prosperity or by conflict and destruction. In this regard, states, international institutions, nuclear security experts, academia, political decision makers and legal advisers will have the historical responsibility to shape further reassurance about the purely peaceful applications of the world's additional nuclear plants investments in nuclear energy power that would be provided by a larger, stronger cooperation with strong support public opinion and awareness.

It is highly critical for essential policies of any nuclear facilities; protection any terrorist organizations attack from achieving their goals of large-scale nuclear violence can best be done by eliminating their access to highly enriched uranium or plutonium. International community should cooperate with IAEA for dependable, secured, adequate protection, thus control measures of such materials are vital. Furthermore,

international community must work together and establish strong partnership for reducing the nuclear terrorism risks to a level as low as possible, while maintaining their control on the states that develop/claim to have developed nuclear energy for military purposes. Physical control over nuclear materials and facilities is also a crucial point of the global agenda. We need better thinking and institutions to deal with physical security and reduce the risk of illicit exports. An even more rigorous application of international norms and standards, as well as tight supervision and inspection on the present and newly emerging facilities may provide useful means in preventing the illegal transfer or theft of nuclear energy. Regarding the changing nature of the terrorism and proliferation networks, states should increase security by ultimately developing new ideas, sharing information, know-how, and creating better institutions, creating more awareness to democratic public opinion control.

Based on the abovementioned parameters, the following recommendations should be made for Turkey:

- ✓ As one of the signatory states of NPT, Ankara should cooperate more with the countries experienced in terms of nuclear energy use such as Twinning Programs developed by the European Union and so on.
- ✓ Within Turkey, a tight and comprehensive collaboration mechanism should be established between state institutions, private & state universities on the nuclear security issues,
- ✓ Public awareness on nuclear security issues should be strengthened within the country through comprehensive education programs,
- ✓ Mutual learning processes should be advanced between Turkey and the countries which build nuclear power plants in Turkey.
- ✓ Turkey should train academicians and experts specifically competent on nuclear security.

REFERENCES

Bayliss, Charlie, "Nuclear Backlash: US to unleash 'OVERWHELMING response' to North Korea if it launches nuke", *The Daily and Sun Express*, 20 October 2016, available at: <http://www.express.co.uk/news/world/723204/North-Korea-US-Ash-Carter-John-Kerry-nuclear-weapons-south-korea-kim-jong-un> .

Caroline Baylon with Roger Brunt and David Livingstone, "Cyber Security at Civil Nuclear Facilities -Understanding the Risks", *Chatham House Report*, Chatham

House, September 2015,
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf.

Berlinger, Joshua , Westcott, Ben , “North Korea Missile Launch: Are US Options Diminishing?”, *CNN Politics*, 29 August 2017,
<http://edition.cnn.com/2017/08/29/politics/north-korea-japan-missile-what-next/index.html>.

Bluth, Christoph, “Offensive Defence in the Warsaw Pact: Reinterpreting Military Doctrine”, *Journal of Strategic Studies*, Vol.18, Issue 4, 1995, pp.55-77.

Cimbala, Stephen J. & Forster, Peter Kent, “The US NATO and military burden sharing: post-Cold War accomplishments and future prospects”, *Defense & Security Analysis*, Vol. 33, No. 2, 2017, pp. 115–130.

Corr, Anders, “Deterrence of Nuclear Terror”, *The Nonproliferation Review*, Vol. 12, No: 1, 2011, pp.127-147, available at:
<http://www.tandfonline.com/doi/abs/10.1080/10736700500208876?journalCode=rnpr20> .

Elisabeth Eaves, “What does "nuclear terrorism" really mean?”, *Bulletin of the Atomic Scientists*, 7 April 2016, available at: <http://thebulletin.org/what-does-nuclear-terrorism-really-mean9309> .

Frost, Robin M., “Terrorism and nuclear deterrence”, *The Adelphi Papers*, Vol.45, No: 378, 2006, pp.63-68.

Fuhrmann, Matthew, “Spreading Temptation: Proliferation and Peaceful Nuclear Cooperation Agreements”, *International Security*, Vol. 34, No. 1, Summer 2009, pp. 7-41.

Fuhrmann, Matthew, Berejikian, Jeffrey D., “Disaggregating Noncompliance: Abstention versus Predation in the Nuclear Nonproliferation Treaty”, *The Journal of Conflict Resolution*, Vol. 56, No. 3, June 2012, pp. 355-381.

Hymans, Jacques E. C., “Theories of Nuclear Proliferation”, *The Nonproliferation Review*, 2010, Vol. 13, No, 3, pp. 455-465.

IAEA News briefs, 7: I, January/February 1992; IAEA Press Release.

“Japan, US Seek to Up Pressure after North Korea Missile Launch”, *Times of Israel*, 29 August 2017, <http://www.timesofisrael.com/japan-us-seek-to-up-pressure-after-north-korea-missile-launch/>.

Jenkins, Bonnie, “Combating Nuclear Terrorism: Addressing Non-state Actor Motivations”, *The Annals of the American Academy of Political and Social Science*, Vol. 607, Confronting the Specter of Nuclear Terrorism, September 2006, pp. 33-42.

Johnson, Jesse, "Trump to speak with Abe and Xi as North Korea nuclear issue looms large", *The Japan Times*, 2 July 2017, available at:
<https://www.japantimes.co.jp/news/2017/07/02/national/politics-diplomacy/trump-speak-abe-xi-north-korea-nuclear-issue-looms-large/#.WZ6QQT5JbIU>.

Joyner, Daniel H, "Recent Developments in International Law Regarding Nuclear Weapons", *The International and Comparative Law Quarterly*, Vol. 60, No. 1, January 2011, pp. 209-224.

Laqueur, Walter, *The Age of Terrorism*, Boston, Little & Brown, 1987.

Lin, Herbert, "War clouds on the Korean peninsula: What would we do if...?", *Bulletin of the Atomic Scientists*, 11 August 2017, available at: <http://thebulletin.org/war-clouds-korean-peninsula-what-would-we-do-if%E2%80%A611016>,

Maerli, Morten Bremer, Schaper, Annette Barnaby, Frank, "The Characteristics of Nuclear Terrorist Weapons", *American Behavioral Scientist*, Vol. 46, No. 6, February 2003, pp.727-744.

"Mapped: The world's nuclear power plants", 8 March 2016,
<https://www.carbonbrief.org/mapped-the-worlds-nuclear-power-plants>.

McLaughlin, Kelly, "Obama slams North Korea's nuclear weapon pursuit and warns Kim 'must face consequences' as he speaks in Seoul after wrapping up his ten-day family vacation in Indonesia", *Daily Mail Online*, 3 July 2017, available at:
<http://www.dailymail.co.uk/news/article-4660572/Barack-Obama-slams-North-Korea-s-nuclear-weapon-pursuit.html> .

Menn, Joseph, "Exclusive: US tries Stuxnet-style campaign against North Korea but failed", *Reuters*, 29 May 2015, <http://www.reuters.com/article/us-usa-northkorea-stuxnet/exclusive-u-s-tried-stuxnet-style-campaign-against-north-korea-but-failed-sources-idUSKBN0OE2DM20150529>.

Meserve, Richard, Rosner, A. Robert, Sagan, Scott D. and Miller, Steven E., "The Nuclear Future", *Bulletin of the American Academy of Arts and Sciences*, Vol. 62, No. 2, Winter 2009, pp. 71-76.

Meserve, Richard A., "The Global Nuclear Safety Regime", *Daedalus*, Vol. 138, No. 4, On the Global Nuclear Future, Vol. 1 , Fall, 2009, pp. 100- 111.

Mesut Hakkı Caşın: " Uluslararası Güvenlik Stratejileri ve Silahsızlanma", Milli Savunma Bakanlığı, Ankara, 1994, s. 88-167.

Mesut Hakkı Caşın:"Illicit Arms Trafficking Crime in International Law ", 5 th Traditional I Law Conference, University of Maribor, Slovenia, 2017, pp.34-57.

Mishra, Sitakanta, "Cyber Threat to Nuclear Installations",
http://www.claws.in/images/journals_doc/SW%20i-10.10.2012.130-133.pdf.

"North Korea's fifth nuclear test", *Strategic Comments*, Vol.22, No. 8, 2016.

O'Neill, Kevin, "The Nuclear Terrorist Threat", August 1997, *Institute for Science and International Security*, available at: <http://www.isis-online.org/publications/terrorism/threat91301.pdf>.

O'Neill, Kevin, "The Nuclear Terrorist Threat", August 1997, Institute for Science and International Security, <http://www.isis-online.org/publications/terrorism/threat91301.pdf>.

Paganini, Pierluigi, "Shocking, a German Nuclear Plant Suffered a Disruptive Cyber Attack", *Security Affairs*, 10 October 2016,
<http://securityaffairs.co/wordpress/52116/security/nuclear-plant-attack.html>.

Phillips, Tom, "Trump vows 'all necessary measures' to protect allies from North Korea, says Abe", *The Guardian*, 31 July 2017,
<https://www.theguardian.com/world/2017/jul/31/trump-vows-all-necessary-measures-to-protect-allies-from-n-korea-says-abe>.

Pilat, Joseph F., "The End of the NPT Regime?", *International Affairs* , Vol. 83, No. 3, Thinking about 'Enlightenment' and 'Counter-Enlightenment' in Nuclear Policies , May, 2007, pp. 469-482.

Ruhl, Lothar, "Offensive Defence in the Warsaw Pact", *Survival*, Vol.33, Issue 5, 1991, pp.442-450.

Savelberg, Ralph, "This is Not the ICBM You Are Looking For; Detailed Analysis Of North Korean Missile", *Breaking Defense*, 6 July, 2017,
<http://breakingdefense.com/2017/07/this-is-not-the-icbm-you-are-looking-for-detailed-analysis-of-north-korean-missile/>.

Scheber, Thomas K., "U.S. Nuclear Policy and Strategy and the NPT Regime: Implications for the NATO Alliance", *Comparative Strategy*, Vol. 26, No: 2, 2007, pp. 117-126.

Schneier, Bruce, "The story behind the Stuxnet virus", *Forbes*, 10 July 2010,
<https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html>.

Shultz, George, P., Perry, William J., Kissinger, Henry A. and Nunn, Sam, "A World Free of Nuclear Weapons", *The Wall Street Journal*, 4 January 2007, p. A15.

Simpson, John, "Nuclear Non-Proliferation in the Post-Cold War Era", *International Affairs*, Vol. 70, No. 1, January 1994, pp. 17-39.

Smith, Martin A., "In a Box in the Corner"? NATO's Theatre Nuclear Weapons, 1989–99", *Journal of Strategic Studies*, Vol.25, No.1 (2002), pp.1–20.

Starr, Barbara, "Latest North Korea missile test renews US talk of military option", *CNN Politics*, 16 September 2017, <http://edition.cnn.com/2017/09/16/politics/north-korea-missile-test/index.html>.

Statement by the Deputy Minister of Foreign Affairs of the Russian Federation, Sergey A. Ryabkov at the 2010 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, May 4, 2010.

Telli, Azime, "Türkiye'nin Nükleer Enerji Açılımının İçerik Analizi: Çeşitlendirme mi, Teslimiyet mi? / Content Analysis of Turkey's Nuclear Energy Initiative: Diversification or Submission?", *Bilge Strateji*, Cilt: 8, Sayı: 14, Bahar 2016, pp.47-75.

Turkey's first nuclear power plant Akkuyu to be operational by 2023", *Daily Sabah Energy*, 3 February 2017, available at:

<https://www.dailysabah.com/energy/2017/02/04/turkeys-first-nuclear-power-plant-akkuyu-to-be-operational-by-2023> .

"Trump issues warning to North Korea over missile launch", *The Australian*, 30 August 2017, <http://www.theaustralian.com.au/news/world/japan-warns-about-north-korea-missile/news-story/7c7b072d6c6200a934da0d297d527a7c>.

Ünal, Ali, "EP call on Turkey to halt Akkuyu Nuclear Power Plant 'not related to hazards'", *Daily Sabah Energy*, 7 July 2017, available at:
<https://www.dailysabah.com/energy/2017/07/08/ep-call-on-turkey-to-halt-akkuyu-nuclear-power-plant-not-related-to-hazards>.

Caşın, Mesut Hakkı, "Pasifik Bölgesinde Kuzey Kore ile ABD ve Müttefikleri Arasındaki Nükleer Krizin Tırmanma Tehdidi Bölgesel Ölçekte Bir Çatışmanın Habercisi Olabilir mi?", *Bilimevi Dış Politika*, Üç Aylık Fikir Dergisi (Ocak-Şubat-Mart 2018), Sayı: 3, pp. 7-32.

Cohen, Zachary and Diamond, Jeremy, "Trump says Pompeo won't go to North Korea, criticizes denuclearization progress", *CNN: Politics*, 25 August 2018, available at: <https://edition.cnn.com/2018/08/24/politics/trump-pompeo-north-korea/index.html> , (Accessed on 19 September 2018).

"DPRK, South Korea Sign Military Agreement Following Summit in Pyongyang", *Sputnik International: Asia & Pacific*, 19 September 2018, available at:
<https://sputniknews.com/asia/201809191068152005-north-south-korea-will-sign-agreement/> , (Accessed on 19 September 2018).

Haas, Benjamin, "North Korea is still developing nuclear weapons, says IAEA", *The Guardian: North Korea*, 22 August 2018, available at:

<https://www.theguardian.com/world/2018/aug/22/north-korea-still-developing-nuclear-weapons-iaea-report-un> , (Accessed on 19 September 2018).

International Atomic Energy Agency Board of Governors General Conference, “GOV/2018/34-GC(62)/12, Application of Safeguards in the Democratic People's Republic of Korea Report by the Director General - Date: 20 August 2018”, available at: https://www-legacy.iaea.org/About/Policy/GC/GC62/GC62Documents/English/gc62-12_en.pdf , (Accessed on 19 September 2018).

“Moscow Regrets US Attempt to Control UNSC Regarding N Korea Sanctions Issue”, *Sputnik International: World*, 19 September 2018, available at: https://sputniknews.com/world/201809191068170235-russia-us-accusations-north-korea-sanctions/?utm_source=push&utm_medium=browser_notification&utm_campaign=sputnik_inter_en , (Accessed on 20 September 2018).

“North Korea Can't Abandon Its Nuclear Weapons – Scholar”, *Sputnik International: Opinion*, 19 September 2018, available at: <https://sputniknews.com/analysis/201809191068162261-north-korea-nuclear-weapons/>, (Accessed on 20 September 2018).

“North Korea continuing nuclear programme - UN report”, *BBC News: Asia*, 4 August 2018, available at: <https://www.bbc.com/news/world-asia-45067681> , (Accessed on 19 September 2018).

“North Korea has not stopped nuclear, missile programme according to confidential UN report”, *The Telegraph: News*, 4 August 2018, available at: <https://www.telegraph.co.uk/news/2018/08/04/north-korea-has-not-stopped-nuclear-missile-programme-according/> , (Accessed on 19 September 2018).

“North Korea's nuclear programme has not been halted, says UN”, *The Guardian: North Korea*, 4 August 2018, available at: <https://www.theguardian.com/world/2018/aug/04/north-koreas-nuclear-programme-has-not-been-halted-says-un> , (Accessed on 19 September 2018).

Nuclear Treaty Initiative, “Countries: Overview – North Korea”, Last Updated: June 2018, available at: <https://www.nti.org/learn/countries/north-korea/> , Accessed on 19 September 2018).

Örmeci, Ozan and Kısacık, Sina, *Rusya Siyaseti ve Rus Dış Politikası: Teorik Çerçeve-Tarihsel Arka Plan-Örnek Olaylar*, (Ankara: Seçkin Yayıncılık, Haziran 2018).

Pak, Jung H. , “The real reason Kim Jong-un wants to declare an end to the Korean War”, *Brookings Series: Trump and Asia Watch – Order from Chaos*, 17 September 2018, available at: https://www.brookings.edu/blog/order-from-chaos/2018/09/17/the-real-reason-kim-jong-un-wants-to-declare-an-end-to-the-korean-war/?utm_campaign=Brookings%20Brief&utm_source=hs_email&utm_medium=email&utm_content=65988763 , (Accessed on 19 September 2018).

“Russia Denies US Accusations of Violating North Korea Sanctions - UN Ambassador”, *Sputnik International: World*, 17 September 2018, available at: <https://sputniknews.com/world/201809171068103700-haley-us-russia-north-korea/> , (Accessed on 20 September 2018).

“Russia Welcomes Inter-Korean Summit – Ambassador to North Korea”, *Sputnik International: World*, 19 September 2018, available at: <https://sputniknews.com/world/201809191068154454-inter-korean-summit/> , (Accessed on 19 September 2018).

“US Must ‘Show Commitment’ to Peace Talks with North Korea – Scholar”, *Sputnik International: Opinion*, 19 September 2018, available at: <https://sputniknews.com/analysis/201809191068150156-kim-moon-meeting-pyongyang-trump-administration/> , (Accessed on 19 September 2018).

Caşın, Mesut Hakkı and Kısacık, Sina, *Avrupa Birliği Enerji Hukuku ve Güvenlik Algılamaları*, (İstanbul: Çağlayan Kitap & Yayıncılık & Eğitim, 2018).

Dyck, Elisabeth “Turkey Starts Construction of its First Nuclear Power Plant”, *International Atomic Energy Agency (IAEA)*, 5 April 2018, available at: <https://www.iaea.org/newscenter/news/turkey-starts-construction-of-its-first-nuclear-power-plant> , (Accessed on 18 September 2018).

“Nicosia to protest construction of Akkuyu nuclear plant”, *Ekathimerini: News*, 5 April 2018, available at: <http://www.ekathimerini.com/227454/article/ekathimerini/news/nicosia-to-protest-construction-of-akkuyu-nuclear-plant> , (Accessed on 18 September 2018).

Örmeci, Ozan and Kısacık, Sina, *Rusya Siyaseti ve Rus Dış Politikası: Teorik Çerçeve-Tarihsel Arka Plan-Örnek Olaylar*, (Ankara: Seçkin Yayıncılık, Haziran 2018).

Presidency of the Republic of Turkey, “We are witnessing a historic moment in terms of energy cooperation between Turkey and Russia”, 3 April 2018, available at: <https://www.tccb.gov.tr/en/news/542/92209/-we-are-witnessing-a-historic-moment-in-terms-of-energy-cooperation-between-turkey-and-russia-> , (Accessed on 18 September 2018).

President of Russia, “Akkuyu Nuclear Power Plant ground-breaking ceremony”, 3 April 2018, available at: <http://en.kremlin.ru/events/president/news/57190> , (Accessed on 18 September 2018).

“Spotlight: Turkey’s first nuclear power plant project goes forth despite setbacks”, *Xinhua: New China*, 4 April 2018, available at: http://www.xinhuanet.com/english/2018-04/04/c_137086211.htm , (Accessed on 18 September 2018).

“Russia willing to build more nuclear plants in Turkey”, *Daily Sabah: Business / Energy*, 6 April 2018, available at: <https://www.dailysabah.com/energy/2018/04/07/russia-willing-to-build-more-nuclear-plants-in-turkey> , (Accessed on 18 September 2018).

Türkiye Cumhuriyeti Enerji ve Tabii Kaynaklar Bakanlığı Nükleer Enerji Proje Uygulama Dairesi Başkanlığı, “Akkuyu Nükleer Güç Santrali Temel Atma Töreni - Enerji ve Tabii Kaynaklar Bakanı Berat Albayrak, Beştepe’deki Cumhurbaşkanlığı Külliyesi’nde düzenlenen Akkuyu NGS’nin temel atma töreninde konuştu.”, 3 April 2018, available at: <https://nepud.enerji.gov.tr/tr-TR/Haberler/Akkuyu-Nukleer-Guc-Santrali-Temel-Atma-Toreni> , (Accessed on 18 September 2018).

“Turkey to Build Its 3rd Nuclear Power Plant on Bulgarian Border”, *Novinite: Sofia News Agency*, 6 April 2011, available at: <https://www.novinite.com/articles/127024/Turkey+to+Build+Its+3rd+Nuclear+Power+Plant+on+Bulgarian+Border>, (Accessed on 19 September 2018).

“Turkey to build third nuclear power plant together with China”, *Trend News Agency*, 8 August 2018, available at: <https://en.trend.az/world/turkey/2938307.html> , (Accessed on 18 September 2018).

“Turkey to Use Russia’s S-400 Air Defense System to Protect Akkuyu NPP – Academic”, *Sputnik International: Opinion*, 28 March 2018, available at: <https://sputniknews.com/analysis/201803281062974799-turkey-russia-s400-akkuyu/> , (Accessed on 19 September 2018).

World Nuclear Association, “Nuclear Power in Turkey”, Updated June 2018, available at: <http://www.world-nuclear.org/information-library/country-profiles/countries-t-z/turkey.aspx> , (Accessed on 18 September 2018).

CRITICAL INFRASTRUCTURE SECURITY PARADIGM AND MODERN PROTECTION POLICIES

Robert RADVANOVSKY

ABSTRACT

Initiated as a concept over 20 years ago, critical infrastructure protection (CIP) originally covered primarily core infrastructure industries which are of vital importance for maintaining society and our way of life. Since then, the number of infrastructure sectors has expanded to include additional industries critical to the continued survival of a country's economic stability.

CIP defined a premise that all infrastructures are interconnected, such that if one infrastructure sector was affected, or worse, compromised, that it could potentially impact other infrastructures. Thus was required to define an all-hazards and holistic approach in addressing strategic and operational issues, threat and attack vectors for maintaining these critically necessary operations. Intrinsically, key factors, such as interdependence, cross-threat correlation, and cascade impact analysis have become extremely important. Security has now taken on a multi-dimensional methodology of which encapsulates all aspects of security including physical, operational, safety and cyber-related activities to address all.

CIP is very important insofar as to its interaction with policy, risk, and political positions, viewing each both separately and combined, to encourage, direct, and maintain continued economic success for not only a single country but for the entire world.

Key Words: Critical Infrastructure, CIP, Convergence

Introduction

For almost 30 years, policy and law makers have been defining, applying and incorporating *critical infrastructure assurance* (CIA) and *critical infrastructure protection* (CIP) methodologies into our society. And yet, it did not appear that long ago that majority of our society never heard these terms, at least not until after the events of 9/11. This now asks the important question of why so much attention is being directed towards our infrastructures.

The answers came shortly after the events that transpired on 9/11 calling for better measures of safeguarding our critical infrastructures when issues of national security and safety were brought to the forefront of industry and government leaders. Since then, many economies have been faced with the conceivable notion that one or more of the many basic necessities that they have determined to expect and depend on may not be available. Imagine a society trying to exist without sufficient clean water, power, transportation, communications, and more.

The accomplishment of safeguarding a critical infrastructure does not depend on any distinctive intelligence collection method or integrated intelligence function. More importantly are the specific diagnostic methodologies that may be used for accessing any vulnerability, while conducting risk evaluations specific to the infrastructure being protected, its remediation, or the mitigation of the risk. This overall process involves communities of scale idealizing in terms of self-protection at a strategic-level, whether it is private industry or government, the premise is similar for whatever organization is implementing such a policy.

It is generally assumed that, with any CIP initiative, the '*bad guys*' are determined adversaries –flexible, creative, resourceful– and are capable in learning how to individually select vulnerable spots while circumventing other areas that may be suitably less protected and/or prone to attack. In many circumstances, modern, sophisticated, or technologically-advanced societies are perfect targets for terrorists; organizations that are not as flexible in their operational practices are equally as targetable.

What is Critical Infrastructure?

The term *critical infrastructure* refers to assets of physical and computer-based systems that are essential to the minimum operations of the economy and government. They include but are not limited to telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.⁸⁶ In any given country, critical infrastructures have been traditionally physically and logically separated systems that had little interaction or dependence upon each other. As technological advances are incorporated to improve efficiencies of industrial operations, infrastructures are becoming increasingly automated and interconnected. These improvements have introduced additional, newer vulnerabilities pertaining to equipment failure, human error, meteorological and other natural causes, as well as physical and computer-related threats. Addressing these vulnerabilities necessitates a greater flexibility, as well as a more holistic approach spanning both public and private sectors so that whatever strategies are implemented protects both domestic and international interests.

⁸⁶ Robert Radvanovsky and Allan McDougall, **Critical Infrastructure: Homeland Security and Emergency Preparedness, Third Edition**, Taylor and Francis – CRC Press (2013), p.45.

Every private-sector organization of a given infrastructure, or government organization or ministry is defining who is responsible for protecting its own infrastructure; each organization should have measures and countermeasures assuring that information is valid and accurate, as well as protecting that information as if it were considered an asset. Part of an assurance process requires routine testing and evaluation of infrastructures, performing vulnerability assessments periodically against physical and computer-based systems, and obtaining expedient and valid authorities to validate those systems. This applies to both the public and private sectors.⁸⁷

What is Critical Infrastructure Protection (CIP)?

The term *critical infrastructure protection* (CIP) pertains to activities for protecting critical infrastructures. This includes people, physical assets, communication, and cyber systems that are indispensable for national, state, and urban security, economic stability, and public safety. CIP methods and resources deter or mitigate attacks against critical infrastructures caused by people (terrorists, other criminals, hackers, etc.), natural disasters (hurricanes, tornadoes, earthquakes, floods, etc.), and hazardous materials accidents involving nuclear, radiological, biological, or chemical substances. Essentially, CIP is about protecting those assets considered invaluable to society that promotes social well-being. CIP is oftentimes considered a reactionary response to threats, risks, vulnerabilities, or hazardous conditions. It does entail some preventative measures as well as countermeasures, but is considered reactive by nature.

CIP has primarily two goals. The first goal can be related back to an alternative way of thinking. By its very definition, a critical infrastructure involves physical and logical systems necessary to support the safety, security, and economic well-being of communities (to paraphrase the growing list of definitions). The second goal is more concerned with the protection of the infrastructure (in its physical and constructional contexts), and whether it is capable of delivering its anticipated services to the community.

What is Critical Infrastructure Assurance (CIA)?

Most asset-protection programs (and their efforts) often begin with determining why something needs to be protected. The first part of this is generally defined in terms of asset identification as well as operational analysis. Various inputs are identified and assigned value based on their contribution to any given system anticipating its desired outputs or results. The second part focuses on threats and assets (things) that can or might disrupt operational processes. These steps become the foundation for such statements whereby risk is incorporated in determining loss or injury of a factor of an asset value, threat, and vulnerability.

Any value associated with a given critical infrastructure may be divided into several parts. The first part involves circumstances in which the critical infrastructure provides

⁸⁷ Ibid.

a unique service within and to a community. This is often the case where infrastructure costs are relatively (or even prohibitively) high, such that the community can only afford one of the installation types. An example that supports this premise might be that it is unlikely that you will see a town of 30,000 inhabitants with a water purification plant able to handle a substantial population increase to some of 150,000 suddenly then decide that it is time to put in place a second similar installation. In this example, the concept of physical security and/or *force protection*⁸⁸ becomes vital, given any potential impacts associated with the interruption, loss, or destruction of that particular infrastructure –in this case, the loss of fresh, drinking water to the local community.

The second part deals with networked configurations; though not within the definition of cyber-related connectivity, this term applies to a network of systems' operations of one or more infrastructures that are interconnected via their operations and associative processes. In a networked environment, an additional layer of protection is possible when leaving the local level as one begins to look at state/provincial, regional, or even national levels. Depending on the nature of the service being provided, the networked environment allows for an application of robustness, resilience, and redundancy to be designed. When one infrastructure suffers a negative impact, the loss of its performance in one area is offset by the remaining elements within the network by either increasing or reallocating its own contributions so as to either reach the desired level of overall performance or, in more extreme cases, reduce the amount of impact associated with the disruption. A *node* may be either a single infrastructure, or if it is distributed, may be one location as part of its overall network. A *conduit* represents the path by which all of the nodes interconnect with one another.

The question becomes whether to protect a single infrastructure or the ability of the networked environment to perform at a level that meets any demands. The truth is that both are needed. Individual nodes and conduits associated with an infrastructure network are intrinsic to that network's ability to function. Additionally, individual nodes operating in isolation must be looked at closely in terms of residual risks allowed into a system that is essentially a single point of failure. An alternative perspective of reality might be that within the critical infrastructure domain there are people (and this should be read in the context of families) that rely on those operating in that field ensuring that services are there when needed.

A range of events illustrates this reality. During the January 1998 ice storm in Canada and the August 2003 blackout that affected much of the northeastern portion of the United States, both circumstances challenged critical functions such that electrical power was not available either to maintain heating and sumps (1998 ice storm), or that refrigeration and heating, ventilation, and air-conditioning systems (2003 blackout). This lack of availability prompted the declared states of emergency, which resulted in organizations putting their business continuity plans into motion while practicing other extraordinary measures. The use of railroad locomotives and generators to supply

⁸⁸ The term 'force protection' describes the use of protective measure taken to mitigate against any hostile actions.

electricity (in response to the ice storm) tends to point toward a lack of electricity being the problem (and not simply a specific electrical transmission line being disrupted).

Consider another example involving a given postal system. Does it really matter what street the mail comes from before it gets to your home? The answer would be "Of course not." What does matter is that your mail arrives at your home (or equivalent) on time and in appropriate (unbroken) condition. The concern sets in when we wonder whether the mail or post is actually being delivered at all –something that affects our paying of bills, receipt of ordered goods, and other forms of communication.

Finally, consider water supply systems. Again, we are less concerned as to whether the water is coming through a central pipe, as opposed to some peripheral parts of the system? We tend to become significantly concerned if the water supply fails to provide water to our homes.

Other examples will tend to follow similar traits as it is the lack of critical services that poses the risk to society. Some might argue that the population is only concerned about protecting critical infrastructure insofar as that protection assures the availability of the service to the public.

This leads to the concept and definition of CIA. The definition of CIP focuses on protecting the nodes and conduits of any given infrastructure that delivers services to their respective communities through force protection. Although CIP tends to focus on an all-hazards approach, it tends to operate at a very basic or local level –for instance, one facility, one road, etc.

CIA instead focuses on a layer higher than CIP, which includes any or all arrangements to shift production around within a given network (or for that matter, even surrounding networks) such that demand is met, even if a local node or conduit is disrupted, either partially or completely. If we are to take our two power-based examples, we would see the difference in the approach. CIP would tend to focus at a very granular level –power production facilities would be protected against various types of physical attacks or hazards. CIA might view the entire power grid, ensuring that the system can detect disruption, shift capacity to meet demand, and ensure that services are being met –often transparently to the consumer. In this context, it might be argued that CIA provides a more holistic view that is actually sought by most CIP professionals.

Functions of a Critical Infrastructure Operation

Defining, using, and maintaining critical infrastructures constitute a process. It is an analytical model or template that guides the systematic protection of the infrastructure. More importantly, it is a reliable decision-making process, a sequential set of methodologies that assists decision makers in determining the possible needs of what methods should be used for whatever is being safeguarded. The process ensures the protection of only those infrastructures upon which survivability, continuity of operations, and their ultimate successes depend on. Thus, these methodologies

safeguard only those infrastructures deemed important and vital for the continued operation of large scale economies.

What most policy makers consider as critical infrastructure has been evolving and is often ambiguous. Almost thirty years ago, the word infrastructure was defined primarily with respect to the adequacy of a nation's public works (water, electricity, waste removal). Sometime in mid-1990s, the growing threat of international terrorism led policy makers to reconsider the definition of an infrastructure in contextual terms relating to national security. In the United States, successive federal government reports, laws, and executive orders have been refined, and the number and types of infrastructure sectors considered to be critical for purposes of national security have been expanded.

What Critical Infrastructure Means to National Security

If critical infrastructure is really about the infrastructure necessary to preserve the safety, security, and economic well-being of citizens, then shouldn't the focus necessarily be on protecting infrastructure or assuring that a given service continues to be delivered as required? Although the former is certainly important, the latter aligns much more closely with the stated goals of CIP.

A given infrastructure at the local level is there to provide some level of contribution into the local system. The sum of these contributions, the ability to coordinate how those services are delivered, and the means of delivering them to their intended recipients may be best described as the capacity of the system.

These three elements (safety, security, and economic well-being) are important because they operate similar to the fire triad (heat, oxygen, chemical reaction). If the infrastructure can generate a significant amount of the service but cannot identify where it is useful or delivered to, then the system has essentially failed. At the same time, a well-coordinated and well-maintained electrical grid that does not have anything sent through it is still failing to meet the final goal. The ability of the system to produce, distribute, and deliver can be described as the system's capacity.

Because of the nature of critical infrastructure, it can be reasonably argued that three imbalances have to be considered. The most serious of these involves a situation where the capacity does not meet the demand (similar to that of economic modeling). This represents a situation where some portion of the population does not receive an expected level of the critical service –such as what occurs resulting from a power failure. The second most serious condition occurs when the capacity exceeds the demand, but leads to an operational response in which the capacity is reduced, leaving the system vulnerable to a spike in demand. This might be exhibited in situations where the private sector is primarily involved in the delivery of the service but due to a surplus of supply, businesses leave the market because they become intolerably unprofitable. The final imbalance is a sustained surplus of capacity.

When an infrastructure is disrupted locally, the disruption loses its ability to continue to provide the expected level of capacity into the overall system. At a local level, the best understanding regarding a loss of capacity would flow from activities less associated with physical security, but instead with *business continuity planning* (BCP). Within BCP thresholds are communicated such that they are used to determine the severity of impacts or losses of key resources, etc. Although BCP generally ends at the edge of the organization's responsibility or mandate, the concept of CIP urges this approach to be executed throughout the organization and into progressively larger systems.

Some care has to be taken to ensure that the quality of service is maintained at a manageable level. What if the final product (e.g. a fuel) fails to reach that level of quality for it to be usable in the system? This aspect of integrity is somewhat different than traditional ones such that the perspective remains status quo insofar that nothing is added, deleted, and only authorized changes are made through well-formed or defined processes which are more closely aligned with traditional views of quality assurance and management.

When something is disrupted, we return to the concept that the availability of the critical service has been reduced. This leads to three important events that are worth noting. The first event involves what the loss or reduction of that service means to the overall system. This revolves around the concept of what consequences arise should the organization fail to meet its goals –again, a power failure, loss of transportation, etc. The second event involves what the loss or reduction of that service means to the internal use or management of inputs that would be normally be used to maintain that level of service delivery. How do the unused inputs survive the impact? Are they perishable or must they be used within a certain timeframe before they are no longer of value? Are they persistent in that they can be stored nearly indefinitely without a loss of value? These factors should generally be included in the basic impact analysis – often in consultation with operations or material management personnel. The third event involves asking how the organization manages the fact that it is no longer consuming those inputs at the same rate. Does this mean that they will stop purchases of future inputs or that they will simply delay the delivery of some? These upstream impacts are also important factors to be considered both in the local impact analysis and also later in the understanding of the impact on the overall system. For those seeking parallels, concepts defined in supply chain management and logistics provide some input.

Generally, at the local level, four classes of impacts are observed. The first are delaying impacts or those that essentially slow the inward flow of something into the system. This concept is seen when warehouses are filled –at some point, the warehouse is full but we still need to store the material. The second involves the concept of lag. This category of disruption describes the condition where something else is slowed down because the necessary amount of inputs is not being received. Finally, at the other end of the spectrum, the system will attempt to balance itself through the push (seeking to

find new demand) and pull (seeking to find surplus capacity that can be aligned against unmet demand) categories.

The concepts of push, pull, lag, and delay are becoming increasingly understood at the local level. This was initially established through bodies of knowledge associated with supply chains and logistics; it then moved into the realm of BCP, and has now become more understood within the realm of CIP. Where the divide currently resides is between the local and regional (small system) levels when you look at the CIP services that have stemmed from such concepts as force protection, infrastructure protection, etc. For the reader, having an awareness that this bridge is likely to be built in the near future has a significant impact on how organizations can prepare and integrate their corporate security, information security [including information technology (IT) security and network security], BCP, incident response (in both the physical and informatics senses of the word), business resumption planning, and disaster recovery planning programs.

When attempting to assure these services, it is most vital to understand how these concepts operate at the small system (regional) level. Consider that each node (or intersection) and each conduit (or channel) can only handle a certain capacity, if there is no release to the surplus demand (e.g. through a release of pressure), then the system simply operates as it is best able to. Beyond that, however, the system begins to clog as the surplus demand that cannot be handled attempts to find other options and, if this is not possible, remains in place.

This concept can be seen in most metropolitan automotive traffic congestion conditions quite clearly. A route can handle a certain number of vehicles in a certain amount of time. When that level is exceeded, the route begins to fill. When the space between intersections is full, vehicles cannot pass through the intersection (or will block the intersection, thus compounding the problem) and the system begins to fill.

What becomes important at this point is the ability to identify that a disruption has taken place, finds alternatives that can release the pressure, and then route (or reroute) the demand onto those alternatives. The release of pressure, if balanced correctly, allows the system to break the cycle of cascading and expanding failure, and regain that delicate operating balance between capacity and demand.

There are two factors that have a serious influence on this. First, what if there is no surplus capacity available in the system? In this instance, the system fills. What is also important to note is that where the system is “full,” it, too, denies further movement through the system. The second factor may be whether surplus capacity within the system can actually be reached from the disruption. The route(s) between them fill as a result of the surplus demand; here, again, we have a situation where the impact is cascading and expanding.

A significant line of research has focused on the concept of interdependencies. Interdependency is where the level of one system’s function or operation is reduced and through this reduction causes an impact to another system. For example, a loss

of fuel production impacts the transportation sector or a loss of electrical power affects telecommunications. For those involved in BCP, the concept of interdependency may appear to be complicated from an operational viewpoint, but is relatively simple to accept at a theoretical level.

When considering interdependencies, one might argue that there needs to be a basic understanding of how the impact flows between or across sectors. These might include, as a basic system of categorization, the following:

- Interdependencies flowing out of one system (host) and impacting an independent system in that the impact does not cycle back onto itself (the host) –henceforth, this would be more of a dependency rather than an interdependency.
- Interdependencies flowing out of one system (host) and impacting a system that provides a direct good or service back into a host system, leads to an elevated rate of deterioration attributable to the initial disruption.
- Interdependencies flowing out of one system (host) and impacting a system that then provides a service to another sector that then has an influence on the host.

In addition to the physical and operational safeguards, the concept of *cyber terrorism* has approached the forefront of many critical infrastructure issues. Outside of Hollywood's extrapolation of potential events, the world has seen clear examples of the results of coordinated cyber attacks in Estonia and Georgia as part of political and military campaigns. We have also seen the specter of groups of cyber criminals operating out of Asia with potential ties to state actors. These issues are of significant concern.

There is now increased recognition within industries and governments that if key resources (and this term is chosen specifically to align with BCP approaches) are connected through Internet-enabled technology, cyber-related threats to those key resources need to be recognized and addressed.

The Great Convergence

Convergence, in very simple terms, may be explained as the gradual integration of physical and logical infrastructure. For those without degrees in architecture (logical or physical), this may be described as the gradual march onto the network-enabled system.

Convergence is really being driven by two interrelated factors. The first factor involves the need for increased efficiency and situational awareness. This comes as a direct result from the need to be increasingly competitive on a global stage. Where North American markets used to be serviced by North American companies, some may argue that the past 25 years have essentially destroyed that concept, particularly with issues associated with supply chains and offshore production. As a result, there is an

increasing intolerance for isolated or stand-alone systems that cannot be expanded as operationally required or as per the will of management.

The second factor involves changes in technology. The current generation of engineers and developers are not particularly enamored with the concept of working with single-purpose, analog systems. The generation that did have to work with that technology is gradually moving on into its retirement years –something that some consider a crisis and others a blessing. The end result, however, is the deployment of key resources using a type of technology that may, if not treated carefully, be subject to the same types of attacks that were present within the context of cyber terrorism.

These two factors, the increasing pressure toward network-enabled systems and also the decreasing supply of those able to work in past logical environments will likely change the face of physical security and enterprise security. The concept of convergence does not simply mean a change in the application of technology; it also requires a change in organizational culture and personal approaches to the issue of security. Some of the basic concepts will, of course, be consistent. As we look at how issues are identified, problems and issues are scoped, challenges are met, and solutions are applied, however, the traditionally divergent IT and physical security communities will be forced back to the same tables. Although the security industry is in for some interesting years as the various elements in these communities go through the normal processes associated, the end result for a given industry may well be worth the effort if both sides remember the primacy of operations.

Convergence will also impact as to how threats are considered within an organization. The all-hazards approach has been front and center in the past –but its application has largely looked at the surface layers of threat. For example, keeping a cyber criminal at bay was a matter of installing a firewall, whereas keeping a prowler out was a matter of locking the door. Today's criminal, however, has access to both tools and with the change of technology, it may well be that the prowler is unknowingly working for the cyber criminal and has access to complex tools specifically conceptualized, designed, and used for defeating security infrastructure through logical means.

The increasing reliance on networks illustrates one potential avenue that could become a sector- or system-wide vulnerability if not led diligently. First, convergence describes a condition by which the physical and asset protection infrastructure is becoming increasingly network enabled. Similarly, operational networks are expanding with new partnerships being formed to streamline delivery of services. The concept of open architecture and common criteria pose a significant challenge at this point. By publishing the open architecture and common criteria, a determined attack planner can identify certain characteristics that are common across the system and can attempt to reverse-engineer those characteristics or criteria in an attempt to determine a weakness. Given that both of these concepts communicate on a global scale, some may surmise that this potential threat vector will likely occur.

But, these same concepts, in their development, also allow for a wide community challenge to the architecture and criteria, thereby reducing a number of the vulnerabilities within the system. The key here is for allowing broad and diligent consultative periods before moving any overall structures into the public domain.

This concept has been a challenge for cryptographers and crypto analysts for quite some time. The result is reasonably simple. The encryption process uses a similar process in the development of new methods of protecting data against unauthorized disclosure or modification. For the critical infrastructure sectors, the principle may be similar. On one hand, the common criteria and open architecture may be globally available, but the specific and detailed information necessary to exploit something at the local level remains hidden from view. Again, this notion hinges on a concept that was rigorously challenged at the front and then monitored in terms of its effectiveness.

Up to this point, our societies have looked at theoretical situations describing critical infrastructure assurance as an overarching, system-based, mission-focused view of how critical infrastructure sectors function. So why does this appear at the relative start of the work? The answer lies in two important factors.

First, the nature of *change* for our societies that occurred as a result of 9/11; many of us did not realize that the changes at that time were a combination of changes that followed the Y2K concerns of 1999.

Second, understanding the business of CIP, homeland security, and similar programs are likely to continue undergoing further changes and refinements. Next, reviewing convergence and its challenges of an evolving hybridization (physical and cyber) of threat, there is also a new pressure to address economic and social issues –and may be argued that the old way of doing business (massive contributions and spending) are about to dramatically alter as we look at renewed fiscal responsibility and restraint. People involved are changing –from the retirement of many of the Cold War era security specialists through the process and systems engineers who defined what we now call *critical infrastructure*.

Today is about looking at the past and seeing what was there, then it is about looking at what is in place today and understanding and questioning the changes that have taken place. Finally, it is about extrapolating, or projecting, that information into the future to best estimate (or perhaps just guessed estimate) what is likely to be.

Today's situation puts the *critical infrastructure protection* and *critical infrastructure assurance* domains at a crossroad.

First, there are significant resource issues. The collapses within the financial and automobile sectors put a significant strain on many economies. Concurrently, the costs associated with foreign wars and its related activities have placed similar strains onto existing economies in terms of debt. Finally, there is the challenge of the reducing tax base caused by an aging population that packs two punches –reduced income through management of fixed incomes (pensions, etc.) as well as lost earnings (in terms of

income tax) and the costs to social security and social support programs. In essence, one might argue that although the cupboard is not bare, we have certainly seen the back of the cupboard and realized that things cannot carry on as they have.

Second, there are significant knowledge base issues. The aging population noted earlier also carries within it a significant portion of the corporate knowledge associated with the infrastructure involved. We are also finally beginning to make the shift from an asset protection mode (some would theorize this was a mitigation response to 9/11) back to an infrastructure assurance mode where a new level of understanding has to be overlaid on top of traditional security and protection approaches. The issues of convergence means that traditionally separate communities will now be forced, through necessity (even if to survive in the economic sense), to interact and cross-pollinate, and as we address these issues within our own community, our adversaries and competitors are working on harnessing opportunities provided in the new structure and our readiness to accept it.

Finally, there is the concept of public-private partnerships. Significant portions of the infrastructure operating outside of federal, or even government, ownership, governments have had to adjust their thinking from a span of control approach (e.g., through the dictating of plans) to a span of influence approach (indicated by the shift toward frameworks).

Conclusion

For those involved in CIP, homeland security, and emergency preparedness, these are exciting times in the research community. The concepts described here are those that are openly researched in the community –concepts that are driving new technologies and approaches to infrastructure management. It also causes friction between communities, particularly those that are firmly attached to rigid doctrines and are unwilling to expand the breadth and depth of those approaches into new areas.

REFERENCES

RADVANOVSKY, R. and MCDOUGALL, A., **Critical Infrastructure: Homeland Security and Emergency Preparedness, Third Edition**, Taylor and Francis – CRC Press, 2013.

SECURING OUR CRITICAL INFRASTRUCTURES

Jane LECLAIR, Scott BURNS

ABSTRACT

Each day hackers become more sophisticated in their attacks on our digital systems, as they threaten not only our businesses, but increasingly, our critical infrastructure. Recognizing the danger to these valuable assets, private organizations operating those systems have joined hands with government agencies to seek ways to mitigate threats to those assets. This chapter will provide an overview of the sixteen identified critical infrastructures and highlight the ongoing efforts to secure them against those with malicious intent.

Key Words: Cyber Security, Critical Infrastructure, Digital Systems, Hackers, Vulnerabilities, Risk, Government Initiatives, FEMA, NIST, Layered Defense, SCADA

The security of the data in our digital systems has become dominated conversations throughout the cyber community in recent years. This conversation is prompted by the ongoing and escalating series of digital breaches that have affected business organizations, educational institutions, healthcare facilities, and government agencies. Hardly a week goes by that the media does not report on yet another cyber breach costing millions of dollars, exposes Personal Identifiable Information (PII), and sullies the reputation of yet another organization or agency.

While the reports of such attacks are important in that they educate and alert the general public to the ongoing security threats, they often neglect a more important aspect, namely the cyber threats faced by critical infrastructure. Although they receive less media attention, attacks on our critical infrastructure are a serious concern. According to a recent survey, almost 90 percent of managers in critical sectors have reported attacks on their organizations, and nearly 50 percent believe that it is likely that a cyber attack on critical infrastructure within the next five years will result in fatalities. Our critical infrastructure is at risk from those with malicious intent, and is by some accounts is more vulnerable than many believe. It must be protected.

As identified by the United States government in Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, there are sixteen types of Critical Infrastructure: the Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector,

Emergency Services Sector, Energy Sector, Financial Services Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, and Water and Wastewater Systems Sector. There are commonalities and differences across each sector.

They have all been identified as essential to the functioning of our society and are in many cases interconnected. However, some are publically owned, while others are private companies, answering only to their stakeholders. As such, each organization has been responsible for its own physical and cyber security, in order to protect its physical and digital assets. This has resulted in a piecemeal system of security measures that has been tailored to the particular needs of each individual sector. While cyber security varies from sector to sector, it generally entails the coordination and interplay of three areas - People, Processes and Technology.

People - We are fallible creatures, and errors in judgment often affect our decisions.

Process - The employees that utilize a digital system must abide by rules and policies that have been established in order to prevent data loss.

Technology - Technology to prevent cyber breaches is a key element of any successful cyber security program.

While each of the critical infrastructure sectors is unique in terms of physical security, they do share commonalities in their cyber defenses: well defined policies, properly trained people, and effective technology. The problem they all face is combining those assets in the correct formula to thwart cyber attacks.

Governmental Initiatives for Critical Infrastructure Protection

The importance of our critical infrastructure cannot be understated. As a guide to protection of critical sectors, the US government developed the "National Infrastructure Protection Plan" (NIPP) – NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience*. This plan details how private organizations and the government can work together to achieve the much-needed security for our critical infrastructure by identifying and managing risks.

Recognizing that a large portion of a nation's critical infrastructure lies in private hands, the government and private organizations joined forces to create partnerships that will work to prevent or seek to reduce attacks on our critical infrastructure. By pooling talents and resources, this government/private sector alliance is working to enhance security and provide rapid responses to events that could cause the collapse of a sector.

A key element in this collaboration is the "The Office of Cyber Security and Communications" (CS&C), which operates within the National Protection and Programs Directorate. The responsibilities of this office include enhancing the resilience, security, and reliability of the cyber security of the country's critical

infrastructure. Coordinating with the private sector, essentially working with ".gov", ".com" and ".edu", the office is primarily concerned with protecting the federal domain of civilian government networks to enhance the security of all critical networks.

In addition, national programs and policies on the security of our critical infrastructure security and resilience are being led by the Office of Infrastructure Protection (IP). This government office has established numerous partnerships across the government and private sector. To assist the private owners of our critical sectors, this Office facilitates vulnerability and consequence assessments in order to help critical infrastructure owners and operators at all levels of government improve their understanding and establish policies and work to reduce risks to those vital sectors. Recognizing that education is a major component of any successful cyber security program, various agencies are working to educate the community by offering numerous independent study courses. These educational offering have been developed by the National Protection and Programs Directorate's Office of Infrastructure Protection. The Federal Emergency Management Agency (FEMA) Emergency Management Institute has made these learning opportunities available to those who will benefit most.

A comprehensive cyber security program entails collaboration across private enterprises, government agencies, and individuals in order to thwart hackers and prevent access to sensitive data, in particular information associated with critical infrastructure. This pooling of individual and corporate talent, combined with the massive resources of the federal government, is a key element of the security system for protecting our critical sectors.

National Institute of Standards and Technology (NIST) – “Framework for Improving Critical Infrastructure Cyber Security”

The economic security and continued well-being of our nation depends on the uninterrupted functioning of our critical infrastructure. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, identifies and defines those sixteen critical sectors. Each sector, despite being intertwined in many regards, has its own cyber security system. Seeking to establish continuity and clear guidelines for enterprises, the White House issued Executive Order 13636 in 2013. The main purpose of the order was to develop of a set of industry-wide standards with associated best practices to assist organizations in managing their perceived cyber security risks. The Executive Order also made the National Institute for Standards and Technology (NIST) responsible for developing the guidelines and working in collaboration with private organizations. The resulting guidelines, published on February 12, 2014, are known as the “Framework for Improving Critical Infrastructure Cyber Security”. The Framework for Improving Critical Infrastructure Cyber Security is composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

The Core of the Framework

This section of the framework includes the common cyber security outcomes, activities and references that are recognized in all the critical sectors. These can be used as staging posts as the organization begins to develop their specific organizational “profiles”.

Profiles

Profiles are extremely useful, as they assist an organization to coordinate and organize their business activities with their corresponding cyber security functions.

Tiers

In managing risk(s), establishing “tiers” enables organizations to improve focus and understanding in regard to the increased risks they face. These tiers range from Tier 1: Partial, Tier 2: Risk Informed, Tier 3: Repeatable, and Tier 4: Adaptive.

The Framework for Improving Critical Infrastructure Cyber Security is not a “cookie cutter” approach to managing cyber security across the various critical infrastructure sectors. The various sectors and private enterprises face unique risks because each is inherently different, and how they choose to apply this framework will also vary in relation to finances. In the absence of a magic bullet to defeat hackers, this framework can act as a guide for coordinating cyber defenses in the critical infrastructure of a nation.

Threat Source-Description

Threats to systems supporting critical infrastructure and federal operations are evolving and growing. Federal agencies have reported increasing numbers of cyber security incidents that have placed sensitive information at risk, with potentially serious impacts on federal and military operations, critical infrastructure, and the confidentiality, integrity, and availability of sensitive government, private sector, and personal information. The increasing risks are demonstrated by the dramatic increase in reports of security incidents, ease of obtaining and using hacking tools, and steady advancements in the sophistication and effectiveness of attack technology.

Successful hacking attacks on financial institutions and various commercial entities have been well documented in the media for some time, and public awareness is relatively established. Consequently, even the most technically savvy users, who do banking and shopping online, do so with at least a degree of trepidation. Conversely, most of us are only vaguely aware of hacking activity against control systems –i.e. the systems that control almost every process in manufacturing and operations today. Control systems such as these are used in the energy industry and other critical infrastructure systems to monitor and control processes associated with the generation, transmission and distribution of infrastructure services. Attacks against energy and manufacturing control systems have been plentiful in recent years – sometimes with devastating consequences.

Recent studies have shown that many control systems are connected in some way to the Internet—often indirectly through a business network. Even the systems that truly have no outside network connectivity are vulnerable. Stuxnet, for instance, was a widely publicized attack against Iranian nuclear enrichment plants that first came to light in 2010. It is important to note that Stuxnet was introduced into an environment that had no direct connection to any outside network. How then were the perpetrators of Stuxnet able to introduce their malicious code into their target environment? One possible explanation is that a trusted employee introduced Stuxnet to internal computing systems via removable media (a USB drive).

Understanding the anatomy of a cyber attack is the first step, as early detection is key to minimizing damage, mitigating risk and reducing the response time. In addition, understanding an attack in terms of its lifecycle can help organizations prioritize, addressing the most persistent, most harmful or most deeply buried threat first.

Defense in Depth

Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets and control systems. Defense in depth is an approach that is used to manage risk with diverse defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can, hopefully, prevent a full breach.

Defense in depth is based on the philosophy that there is no real possibility of achieving comprehensive security by implementing any collection of security solutions. Rather, technological components of a layered security strategy are regarded as preventative measures that hinder the progress of a threat, until either it ceases to pose a threat, or some additional resources—not strictly technological in nature—can be brought to bear. Defense in depth is a more holistic approach that addresses a broader range of possibilities, such as physical theft followed by forensic recovery of data by unauthorized persons, or incidental threats as a result of dangers that do not specifically target the protected systems. Components of defense in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection, and biometric verification. In addition to electronic countermeasures, physical protection of business sites along with comprehensive and ongoing personnel training enhances the security of vital data against compromise, theft, or destruction.

Defense in depth minimizes the likelihood that the efforts of malicious hackers will succeed. If a hacker gains access to a system, defense in depth minimizes the adverse impacts and gives administrators and engineers time to deploy new or updated countermeasures to prevent recurrence. Defense in depth is a process, not a product. It's a proactive approach to thinking about security from the inside out. Certain architectural approaches such as centralized security overlays lend themselves well to solving internal security problems. Security is an ongoing process, and constant vigilance and user awareness play equally important roles in building strong security models.

The Defense in Depth Approach for the Electric Utility Industry

Developing a Defense in Depth approach to cyber security entails building a hybrid, multi-layered security strategy that provides holistic security throughout an industrial enterprise. There are a number of key steps to building a comprehensive approach to defensive security approach, include the following:

Security Plan: Policies and procedures that cover risk assessment, risk mitigation and methods to recover from disaster.

Network Separation: Separating industrial automation and control system from other networks by creating demilitarized zones (DMZ) to protect the industrial system from enterprise network requests and messages.

Perimeter Protection: Firewalls, authentication, authorizations, VPN (IPsec) and antivirus software to prevent unauthorized access.

Network Segmentation: Containing a potential security breach within the affected segment, by using switches and VLANs to divide the network into sub-networks and by restricting traffic between segments. This helps contain malware impact to a single network segment; thus limiting damage to the entire network.

Device Hardening: Password management, user profile definition and deactivation of unused services to strengthen security on devices.

Monitoring & Update: Surveillance of operator activity and network communications. Regular updates of software and firmware.

The defense in depth approach is considered a layered strategy because it employs defensive controls from overlapping and complementary areas. For example, the Network Segmentation and Monitoring and Update concepts are combined to form a defensive architecture that is more robust than each concept implemented individually. Monitoring systems can be standalone, but many are connected to the plant business network so that all necessary groups have access to this data. A firewall can be used as an isolation device between the monitoring and business network. These are not 100% reliable protections because they allow two-way communications. The firewall has internal rules to determine what information may pass through, but these rules can be breached by hackers. The preferred solution is to combine firewalls with Network Segmentation through the use of a device known as a data diode, which only allows unidirectional communication. Information can flow out of the monitoring network into the business network, but reverse flow is not allowed. In nuclear power plants, the monitoring systems use a data diode to connect to the business network. Control systems are segmented and protected and no outside access to these critical systems is possible.

Emerging Trends

Modern society relies heavily upon complex and widespread electric grids. In recent years, advanced sensors, intelligent automation, communications networks and

information technologies have been integrated into the electric grid to enhance performance and efficiency. Integrating these new technologies has resulted in more interconnections and interdependencies between the physical and cyber components of the grid.

We live in an era of uncertainty and increasing vulnerability. In our electronic age of complex, interconnected infrastructures and open societies, protection from terrorists, natural disasters, systems failures, or other threats cannot be guaranteed, despite all the resources that may be poured into preventative, defensive, and offensive measures. Moreover, practitioners, policymakers, and researchers are only beginning to understand at a superficial level the many and multi-layered interdependencies among these entities, and the vulnerabilities associated with them under the various scenarios that can cause direct and indirect cascading affects, including regional paralysis with far-reaching economic and political consequences. Because, sooner or later, protection will inevitably fail, the focus must be on cost-effective mitigation measures, damage control, and reconstitution.

A “smart grid”, one response to this situation, can strengthen the connection between information and communication technology (ICT) and advanced control systems. The synergy between the physical power network components, communication network, and cyber components may revolutionize grid efficiency and performance, but it also adds new cyber access points increases the risk of physical damage cyber intruders. Moreover, interdependencies between electric transmission networks and distribution networks increase vulnerability, and therefore must therefore be evaluated both from the physical as well as the cyber space and interdependence perspective.

REFERENCES

BENNETT, C., "Study: Cyber Attacks up 48 Percent in 2014",
<http://thehill.com/policy/cybersecurity/221936-study-cyber-attacks-up-48-percent-in-2014>, 2014.

DRINKWATER, D., "Study: Critical Infrastructure Attacks Often Result in Physical Damage", <http://www.scmagazineuk.com/study-critical-infrastructure-attacks-often-result-in-physical-damage/article/427267/>, 2015.

GANDEL, S., "Lloyd's CEO: Cyber attacks cost companies \$400 billion every year",
<http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>, 2015.

GRANVILLE, K., "9 Recent Cyber Attacks against Big Businesses",
http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0, 2015.

National Institute of Standards and Technology, "*Framework for Improving Critical Infrastructure Cyber Security*",
<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>, 2014.

Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities,
<https://scp.nrc.gov/slo/regguide571.pdf>

Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations,
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

The White House, "*Cyber Security – Executive Order 13636*",
<https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636>, 2013.

United States Department of Homeland Security, "*The National Infrastructure Protection Plan*", <http://www.dhs.gov/national-infrastructure-protection-plan>, 2015.

United States Department of Homeland Security, "*What is Critical Infrastructure?*",
<http://www.dhs.gov/what-critical-infrastructure>, 2015.

CYBER SECURITY POLICIES FOR CRITICAL ENERGY INFRASTRUCTURES IN KOREA - FOCUSING ON CYBER SECURITY FOR NUCLEAR POWER PLANTS

IL SEOK (LUKE), OH

SO JEONG, KIM

ABSTRACT

Risks shall be allocated to a person, an institute or an organization which would have a power to control them. Cyber risks including cyber attacks, cyber threats and cyber crimes shall not be assigned to a person, institute an institute or an organization because cyber space shall not be controlled. Cyber security, responding and making measures, standards and policies against cyber risks, shall be regarded as public good and under market failures. A person, an institute or an organization will not be willing to take actions against cyber risks. Therefore, cyber risks shall be allocated to a state. In Korea, to protect critical information infrastructures from cyber risks, "Critical Information Infrastructure Protection Act" has been enacted since 2001. According to the Act, cyber risks on critical information infrastructures shall be allocated to the Management Agencies, and the Article 25 of the Act shall describe duties of a state to support the Management by providing equipment, technical assistance and other supports to protect critical information infrastructures. However, this article shall not illustrate any detailed procedures and programs. Therefore we recommend amending the title of this article to "governmental budget support to the Management Agencies" and insert clauses with which state shall provide "government subsidies" and "loans" directly to the Agencies. Furthermore, we recommend establishing Mutual Benefit Association of the Agencies to support each other. We also recommend the article 7(technical assistance) of the Act should be amended to allow NCSC to make technical assistance for MAs, and a new clause should be inserted to the article 7-2 which mandates a duty for NCSC to maintain and protect personal information comprised in the critical information infrastructures, with the other new clauses that National Assembly shall control the technical assistance activities made by NCSC, to defend personal information.

Cyber attacks against nuclear power plants may cause huge damages not only human beings but also whole livings and environmental damages. Therefore comprehensive security measures shall be established in considering system life cycle, physical protection and work process according to the Nuclear Protection and Prevention Act. These security measures shall be performed by Korea Institute of Nuclear Nonproliferation and Control (KINAC) supervised by Nuclear Safety and Security

Commission (herein after “NSSC”). The KINAC/RS-015 is to establish efficient prevention, detention, response system against cyber attacks, and minimize effects and results of cyber attacks which seek to sabotage on nuclear facilities and illegal transportation of nuclear materials

When computer and network systems in nuclear power plants should be designated as critical information infrastructure, they shall be governed not only Nuclear Protection and Prevention Act but also CIIP Act. To resolve these duplications, we recommend CIIP Act should be amended to have a specific provision describing that nuclear power plants shall be governed and secured from cyber attacks according to the Nuclear Protection and Prevention Act. However preventing and responding cyber attack for nuclear power plants shall be compromised with nationwide policies and standards. Therefore CIIP Act shall be amended to make a process that Chairman of the NSSC shall make reports on their activities related to cyber security for nuclear power plants by periodically. Along with the amendment, the Presidential Decree of CIIP Act shall be amended that the Chairman of the NSSC shall be a member of the Committee for Critical Information Infrastructure Protection.

Key Words: Critical Information Infrastructure, National Cyber Security Center, technical assistance, governmental budget support to the Management Agencies Critical Information Infrastructure Protection Act, Nuclear Protection and Prevention Act, Technical Standards(KINAC/RS-015)

1. Introduction

Korea has suffered several critical cyber attacks such as 1.25 cyber crisis in 2003, 7.7 and 3.4 DDoS attacks in 2009 and 2011, 3.20 NH Banking Hacking in 2011, 3.20 and 6.25. cyber attack in 2013.

In Korea, to protect critical information infrastructures from cyber threats and attacks, “The Critical Information Infrastructure Protection Act (herein after “CIIP Act”)” has been enacted since 2001. According to the Act, the Critical Information Infrastructure Protection Committee has been established under Prime Minister’s Office. The committee has compromised CIIP related activities conducted by several governmental authorities. Under the Act, 'National Cyber Security Center (NCSC) of National Intelligence Service(NIS)' and 'Ministry of Science, Information and Communications Technology and Future Planning(MSIP)' have also taken great roles in CIIP activities. Especially NCSC, which has developed advanced technologies and trained experts, has practically coordinated CIIP related governmental activities. Following the Act, about 300 facilities including nuclear power plants systems,

transportation systems and commercial banks networks have been designated as Critical Information Infrastructure(CII).⁸⁹

Protecting energy infrastructures from the cyber attacks shall be enforced by the measures, plans and responding processes described in the Act. Before the cyber attacks on nuclear power plants happened in last winter season, main issues on nuclear energy infrastructure were checking and reviewing safety operation of nuclear power plant, and appropriation of prolonging old nuclear power plant reactor's operation. However, after the cyber attacks, Korean society has requested establishing more profound and specific measures to protect nuclear energy infrastructure from cyber attacks. Following these requests, legislators of National Assembly in Korea, have proposed many bills to amend "the Act on measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters (herein after "Nuclear Protection and Prevention Act")".

In this article, we would like to explore the cyber attacks against the nuclear power plants happened in last winter season, to review system and networks in nuclear power plants, cyber security structure focusing on Nuclear Protection and Prevention Act, and to study cyber security standards for nuclear power plants with recently published KINAC/RS-015. Then we also explore CIIP Act with a view point from the risk allocation by designation of CII, pre-CII protection measures and post-CII protection measures.

Based on these explorations, we finally propose and recommend a proper measures and amendments to establish more practical practice to protect nuclear energy infrastructures including nuclear power plants from cyber attacks.

2. Cyber Security for Nuclear Power Plants in Korea

2.1 Cyber Attacks on Nuclear Power Plants

In December 2014, South Korea's nuclear power plant operator, Korea Hydro and Nuclear Power(KHNP) said its computer system have been breached and resulted in the leak of personal details of 10,000 KHPN workers, designs and manuals for at least two reactors, electro flow charts and estimates of radiation exposure among local residents.⁹⁰ The cyber attacks were made between Dec. 9 and 12 by sending 5,986 phishing emails containing malicious codes to 3,571 employees of the nuclear plant

⁸⁹ IL SEOK, OH, Comment on Cyber Security Issues in Korea, International Cyber Security Expert Round Table Meeting in National Assembly Research Service hosted by NSRI and JeJu Peace Institute(May 8, 2015). However, about 70% of the CIIs are in public and governmental sectors, which is very different from U.S. situation which over 70% of CIIs are in private sectors.

⁹⁰ <http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack>

operator.⁹¹ A hacker who leaked information about South Korea's nuclear plants online demanded money for not handing over sensitive information about the plants to other countries, and he had posted files, including documents about the country's indigenous advanced power reactor, on Twitter.⁹² The malicious codes used for the nuclear-operator hacking were the same in composition and working methods as the so-called 'kimsuky' that North Korean hackers use.⁹³ Fortunately, control systems at nuclear plants have not been harmed by the cyber attacks by hackers, but nevertheless KHNP is increasing its security efforts to defend against possible additional attacks⁹⁴ The hacker could not have accessed classified information because its internal server has been isolated since last year.⁹⁵ No critical data was disclosed and the emails, which also aimed at obtaining remote control access of computers, were largely unsuccessful.⁹⁶ Therefore South Korean government has concluded that the hacker has an intention to cause confusion into Korean Society not to disclose and leak confidential data or materials.^{97 98}

2.2 Necessity of cyber security for nuclear power plants

Along with the technical development of computer and network systems, cyber threat and attacks against nuclear power plant have also increased. Nuclear digital system is in nature different from general information and telecommunication systems. It shall be need to response simultaneously within an order time serviced by 24hours and 7days with 30 to 40 years. Cyber attacks against nuclear power plants may cause huge damages not only human beings but also whole livings and environmental damages. Therefore comprehensive security measures shall be established in considering system life cycle, physical protection and work process. The measures shall include security measures for system developers, system maintain staffs, third party contractor and inside workers.

⁹¹ <http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317>

⁹² <http://www.ibtimes.com/hacker-who-posted-south-korean-nuclear-plants-information-online-demands-money-1845838>

⁹³ <http://www.foxnews.com/world/2015/03/17/south-korea-points-finger-at-north-korea-in-nuclear-operator-cyberattack/>

⁹⁴ <http://www.pcworld.com/article/2864072/south-korea-nuclear-operator-strengthens-security-system-against-cyber-attack.html>

⁹⁵ <http://www.ibtimes.com/hacker-who-posted-south-korean-nuclear-plants-information-online-demands-money-1845838>

⁹⁶ <http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317>

⁹⁷ White Paper on National Information Security(2015), p.

⁹⁸ Regarding general description of this case and it's political, legal and technological implication, refer this : So Jeong KIM, Christopher Spirito, Eneken Tikk-Ringas, "Multinational Confidence Building Measures (CBMs) in support of Nuclear Safety and Security", International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, Vienna, Austria, 2015-06-01 - 2015-06-05

2.3 System and networks in nuclear power plants

Nuclear power plants shall usually have developed 3 levels of systems and networks such as 1) internet network, 2) intra network and 3) independently blocked network. As the internet and intra network are separated, workers and staffs shall have a work only within the intra network. When they want to access with internet they shall use only internet network separated from intranet work. This cause several inefficiency and inconvenient but it shall be helpful to increase security. Intra network shall be connected with the independently blocked network controlling nuclear reactor, turbine control system, main computers and operating computers, however the independently blocked network shall transfer only simple operation information to intra network. Therefore it can be said that in fact the independently blocked network closed to intra networks.

2.4 Structures on Safety and Security for Nuclear Power Plants

In Korea two major Acts, 1) Nuclear Safety Act and 2) Nuclear Protection and Prevention Act, have regulated security issues against nuclear power plants. The purpose of the Nuclear Safety Act is to provide for matters concerning safety managements in research, development, production, use, etc. of nuclear energy, in order to ensure the prevention of disasters resulting from radiation and to contribute to public safety. The purpose of Nuclear Safety Act is to ensure safety and trustfulness of the nuclear energy, it shall not include regulation against cyber security issues related to nuclear power facilities.

However the purpose of the Nuclear Protection and Prevention Act is to strengthen the protection system of nuclear facilities to guard against an increase of the number of nuclear facilities or new threats such as terror and sabotage, and to establish legal and institutional frameworks for an efficient radiation disaster management system. According to this Act, guidelines and regulations controlling illegal transfer of nuclear materials and sabotage by cyber attacks shall be presented and regulated.

Nuclear Safety and Security Commission (herein after “NSSC”) shall be established directly under Prime Minister, as a central government organization and it shall be composed of 9 commissioners including 1 chairperson who shall be the standing member of the commission after being appointed with the consent of the National Assembly. NSSC shall 1) secure the highest level of nuclear safety, 2) protect nuclear facilities from both internal and external threats, such as terrorism, 3) strengthen emergency system for any nuclear emergency or accidents, and 4) comply with international standards for the peaceful use of nuclear energy.⁹⁹

⁹⁹ <http://www.nssc.go.kr/nssc/en/c1/sub1.jsp>.

Every nuclear business operator shall obtain approval from NSSC for the 3 following matters: 1) Physical protection facilities and installations for "Protection against the illicit transfer of nuclear materials", "Measures to locate and collect lost or stolen nuclear materials", "Prevention of sabotaging nuclear facilities, etc.", and "Measures against radiological effects resulting from sabotaging nuclear facilities, etc."¹⁰⁰, 2) Regulations for the physical protection of nuclear facilities, etc. (hereinafter referred to as "physical protection regulations"), 3) Plans for measures against the illicit transfer of nuclear materials and threats to nuclear facilities, etc. (hereinafter referred to as "protection emergency plan").¹⁰¹ When an operator wants a slight alternation described by Prime Minister's Regulation, he or she shall file an alternation report to NSSC. Cyber security matters shall be included into the each above 3 matters. Physical protection of nuclear facilities operated by nuclear business operator shall be under inspection of NSSC.¹⁰² When NSSC found certain results such as violation of physical protection regulation and insufficient emergency protection measures by the operators under the inspection, NSSC shall order the nuclear business operator to correct them.¹⁰³

NSSC also shall assess the threats against nuclear facilities and establish design based threat with every 3 years to implement physical protection measures.¹⁰⁴

2.5. Korea Institute of Nuclear Nonproliferation and Control (KINAC) and its RS-015

2.5.1. KINAC

The Korea Institute of Nuclear Nonproliferation and Control (hereinafter referred to as "KINAC") shall be established in order to take steps to ensure the safeguard of nuclear energy facilities and nuclear materials and to efficiently perform the work of controlling the import and export of the nuclear materials.¹⁰⁵ KINAC shall 1) conduct regulatory work on nuclear material accounting and control, 2) implement a comprehensive safeguards agreement (CSA), the additional protocol(AP) and other relevant activities, 3) implement Import & Export control governing nuclear materials and related technologies, 4) review and Inspect the physical protection status of nuclear material and facilities, 5) cooperate with the International community with regard to nuclear nonproliferation and nuclear security, 6) train, Educate and Conduct R&D activities in the area of nuclear nonproliferation and nuclear security, 7) analyze the nuclear

¹⁰⁰ Article 3 Para 2 of the Nuclear Protection and Prevention Act

¹⁰¹ Article 9 of the Nuclear Protection and Prevention Act

¹⁰² Article 12 Para 1 of the Nuclear Protection and Prevention Act

¹⁰³ Article 12 Para 2 of the Nuclear Protection and Prevention Act

¹⁰⁴ Article 7 of the Presidential Decree of the Nuclear Protection and Prevention Act

¹⁰⁵ Article 6 the Nuclear Safety Act

activities of North Korea and neighboring countries, and 8) develop nuclear nonproliferation and security policies.¹⁰⁶

NSSC shall entrust 1) threat assessment, 2) review for the approval for above “physical protection facilities and installations”, “physical protection regulations” and “protection emergency plan”, and 3) inspections on physical protection, to KINAC.¹⁰⁷ Based on the entrustment of the NSSC, KINAC has developed standards on cyber security on nuclear power facilities. Especially after recent cyber attacks and hacking against nuclear power plant, KINAC has published KINAC/RS-015.

2.5.2. KINAC/RS-015

2.5.2.1 Purpose and target of the KINAC/RS-015

The KINAC/RS-015 is to establish efficient prevention, detention, response system against cyber attacks, and minimize effects and results of cyber attacks which seek to sabotage on nuclear facilities and illegal transportation of nuclear materials.

KINAC/RS-015 shall have be applied to Critical Digital Assets (CDAs) which implements Safety, Security, Emergency Preparedness(SSEP) functions and makes effects on SSEP functions when cyber attacks happen. To prevent and protect illegal transfer of nuclear materials, KINAC/RS-015 shall be applied to security networks, composed of access control system, and computers and servers covering intrusion detection system. KINAC/RS-015 shall be also applied to control networks, composed of reactor control system, detection system, protection system, technical safety system, and computers, servers, PLC and DCS in diversity system.

2.5.2.2 Main Contents of Technical Standards(in KINAC/RS-015)

First, nuclear business operators shall make a cyber security team(CST) which shall be independent and separated from operation. They also shall describe explicitly role and liabilities of the each team members. Second they shall identify critical digital assets. Before identifying CDAs, they shall identify critical systems by doing initial consequence analysis which shall be applied to whole operating systems, communication systems, networks and support systems in nuclear power plant, deciding critical systems which would conduct adverse impact against SSEP. They shall identify critical systems which have implemented SSEP functions or SSEP functions would have defended on, or made adverse impacts on implement of SSEP functions. When a system has provided a way of access process or assist necessity

¹⁰⁶ http://www.kinac.re.kr:8181/eng/about/about2_3.do

¹⁰⁷ Article 7 of the Presidential Decree of the Nuclear Protection and Prevention Act

system, it shall be a critical system. When a system has not implemented these functions and there is no need to protect the system as a necessity it shall not be a necessity system.

Second nuclear operators shall identify CDAs. CDA shall be a component of critical system, which shall protect critical systems when cyber attacks happened, or shall be connected with critical system directly or indirectly. Digital assets which shall 1) implement SSEP functions, 2) make adverse impacts or would make adverse impact against critical system doing SSEP function or CDAs, 3) digital assets which supply access way for critical system doing SSEP or CDAs, 4) digital assets which support critical system or CDAs, 5) CDAs which shall protect above systems from cyber attacks defined in design based threats.

Third they shall establish a Defense-in-Depth strategy. Under this strategy they shall make classifications with cyber security degrees to protect core digital assets. The cyber security degrees are composed of level 1 to level 4, and transfer among the levels shall be controlled.

Forth they shall apply 101 cyber security measures to core digital assets. These cyber security measures are composed of technical, operational and management security measures. Technical security measures shall be composed of access control, supervision and liability, security on systems and telecommunications, user identification and certification, system enhancements such as patch. Operational security measures shall be composed of controlling media, personal security, enhancing confidentiality of system and information, maintenance, physical and environmental security, protection strategy and responding incidents. Preparing emergence plan, training and education shall be also composing operational security measures. Supply network control, security design, development and acceptance test, and managing vulnerabilities shall belong to maintenance security measures.

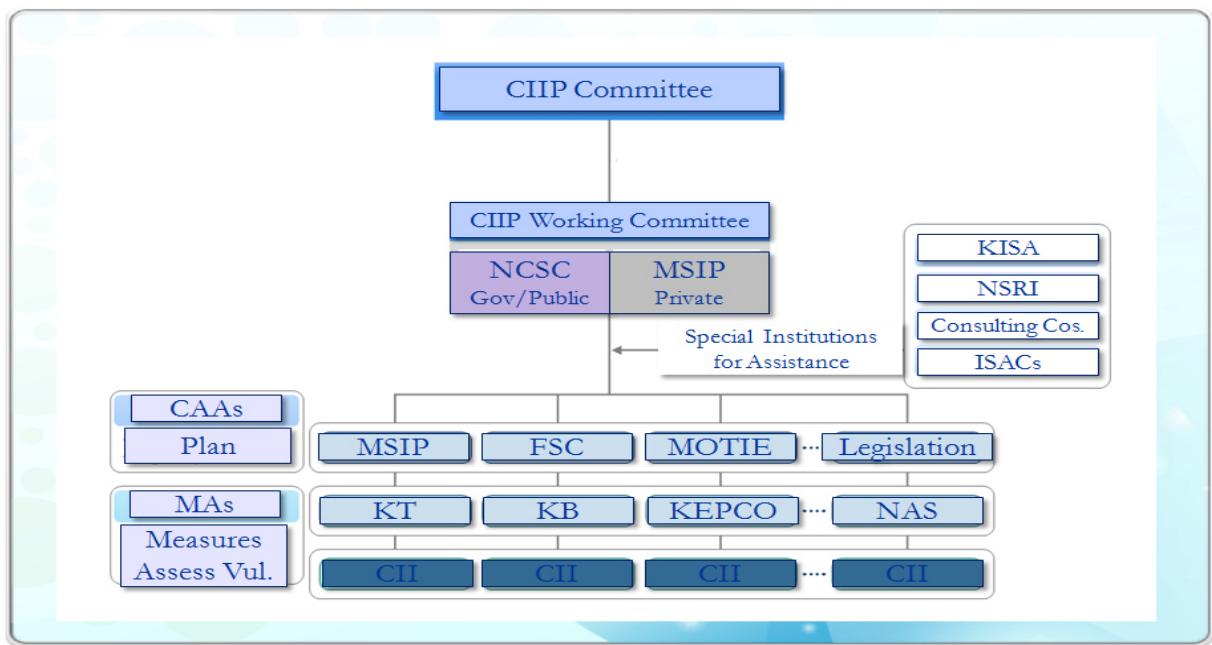
Finally nuclear business operators shall maintain and sustain the cyber security programs with sustainable detection and assessment, and analyzing vulnerabilities. To maintain cyber security program, the operators shall establish cyber security program, integrate it, maintain continuously, review security program, change control when necessary, and record retentions.

3. Critical Information Infrastructure Protection in Korea

3.1 Overview

The Act describes proper protections with pro- and post-measures. As a first step for pro-protection measures, the Act describes a central administrative authority(CAA) has an authority to designate information infrastructures to CIIs operated by

management agency(MA)s under its control. A CAA may establish the detailed assessment standards and guidelines for designation and shall deliver these to MAs under its supervision. NCSC and MSIP may recommend a CAA to designate a specific information infrastructure as a CII with the new provision of recommendation for designation.



The second step for pro-protection measures is analysis and evaluation of vulnerabilities. According to CIIP Act, a MA shall analyze and evaluate the vulnerabilities of CIIs under its control on a regular basis. Based on the results from the analysis and evaluation of vulnerabilities, the MA shall establish and implement protection measures. NCSC, MSIP and Ministry of National Defense(MND) may review whether a MA properly implements measures to protect CII or not. A relevant CAA shall establish and implement plans for protecting CII within its authority by integrating and coordinating the measures submitted by the MAs under its supervision. Post-CII protection measures are composed with 3 parts, 1) notification, 2) resilience measures and 3) technical assistance. A MA shall, when it recognizes that the occurrence of intrusion incidents lead to the disturbance, paralysis or destruction of CII under its control, notify relevant administrative authorities and law enforcement authorities of such facts. A MA shall take necessary measures to make resilience and protect CII in a swift manner when intrusion incidents occur. MAs may also request technical assistant, if it is necessary, to the NCSC, MSIP or specialized institutions prescribed by Presidential Decree.

3.2 Designation of CII

3.2.1 CII

Information Infrastructure means an electronic control and a management system related to the national security, administration, defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article 2 para. 1 subpara. 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. An information infrastructure shall be a critical information infrastructure after it shall be designated as a CII.

3.2.2 Designation of CII

3.2.2.1 Authority for Designation

Protection measures, protection plans and technical assistance described in CIIP Act shall be applied to an information infrastructure, after it shall be designated as a CII. The Act describes a CAA has an authority to designate information infrastructures to CIIs operated by MAs under its control. When a CAA performs the designation, it shall establish its own assessment standard on the designation and make a notice it to the MAs.¹⁰⁸ The Act and the Decree guarantee CAAs to have autonomy in designation of CIIs, because CAAs would be aware of the unique features and specific circumstances related to CIIs under its control.

However CAAs, based on its autonomy in designation of CIIs, would like to designate so many information infrastructures as CIIs, because it could not have enough experts and budgets to identify CIIs among information infrastructures under its control and it would likely to avoid liability from no designation of CIIs. Sometimes CAAs, would not designate or delay the designation, because making compliance with the Act would be burdensome. To prevent surplus designation of CII, the Act makes a process that the Committee shall have a power to make a decision on whether the CAA's designation should be proper or not. To respond no designation or delay, the Act has a provision on the Recommendation for Designation.

3.2.2.2 Standards and Guidelines

A central CAA may designate an information infrastructure operated by a MA under its authority, which is deemed to require protection from electronic intrusions, as a CII.¹⁰⁹ When a CAA designate a CII, it shall take into account these standards; i) the national and social importance of duties performed by the MA; ii) the agency's

¹⁰⁸ Article 8 of the Act and article 14 of Presidential Decree.

¹⁰⁹ Article 8 para.1. of the Act.

dependence on the information infrastructure; iii) the inter-connection with other information infrastructures; iv) the areas and extent of damage caused by intrusion incidents to the national security, economy and society, if any; v) the probability of intrusion incidents and the easiness of resilience thereof.

A CAA may establish the detailed assessment standards and guidelines for designation and shall deliver these to MAs under its supervision.¹¹⁰ MAs shall make task force for the performance of the assessment for designation, and the task force shall select designated units and areas of the detailed infrastructure facilities, according to the standards and guidelines.

3.2.3 Recommendation for Designation

Although CIIP Act was enacted, CAAs were very reluctant to designate CIIs, because designation would bring a great burden for CAA and MAs to comply requirements and duties described in the Act. In April 2001, 4 CAAs designated 23 facilities as CIIs and in 2002, 5 CAAs designated 66 facilities. A CAA, Ministry of Information and Communication at that time, designated 7 facilities in 2004. In 2005, a CAA, Central Election Commission, designated 1 facility and in 2006 the Ministry of Information and Communication at that time, designated 5 facilities. Because CAAs had their own authority to designate CIIs, based on its own decision, there was no measure to force CAA to make designation. Therefore it was needed to make proper measures for CAAs to encourage enforce their designation authority.

Under this background, the CIIP Act revised in 2007 to introduce new provision of recommendation for designation. According to the provision, NCSC and MSIP may recommend a CAA to designate a specific information infrastructure as a CII.¹¹¹ In that case NCSC and MSIP shall require CAA to submit data on the relevant information infrastructure, when necessary for making a recommendation¹¹² When CAAs had received the recommendation for designation, they shall designate CIIs following above designation procedure. In other words, when CAA received the recommendation, it shall make decision on the designation following above designation procedures and notify the result to NCSC or MSPI within 60days.¹¹³ To make a recommendation, NCSC and MSIP shall establish Research Task Force to review the necessity of designation, considering above 5 designation standards.¹¹⁴ Before making a recommendation, NCSC and MSIP may consult with the MA which operates a specific information infrastructure and CAA supervising the MA.¹¹⁵ NCSC

¹¹⁰ Article 14 para. 1 of the Presidential Decree.

¹¹¹ Article 8-2, para.1. of the Act.

¹¹² Article 8-2, para.2. of the Act.

¹¹³ Article 16-2 para.3 of the Presidential Decree.

¹¹⁴ Article 16-2 para.1 of the Presidential Decree.

¹¹⁵ Article 16-2 para.2 of the Presidential Decree.

and MSPI shall describe necessary matters related to establishing and operating the Task Force.¹¹⁶

3.2.4 Revocation of Designation

When a MA abolishes, suspends or changes its business operations, the related CAA may revoke the designation either ex officio or upon request of the MA.¹¹⁷ When CAA is likely to revoke the designation, it shall submit this for deliberation by the Committee and in such a case, the Committee may hear MA's opinion on the revocation.¹¹⁸ When the Committee makes an agreement for the revocation, CAA make a notification of the revocation to MAs and publish this in the official gazette. However, CAA may not publicly announce it, after deliberation by the Committee, when necessary for guaranteeing national security.¹¹⁹ Compared with designation, revocation may be possible when a MA abolishes, suspends or changes its business operations. Therefore it is needed to revise the Act that a revocation shall be happened based on the above 5 designation standards. Furthermore the Act shall be revised to enforce the MA's interest on related to revocation, by describing Committee hearing to be mandatory.¹²⁰

3.3 Evaluating Vulnerabilities and Establishing Protection Plans

3.3.1 Analysis and Evaluation of Vulnerabilities

3.3.1.1 Introduction and period

Because of increasing interdependency combined with greater operational complexity, CIIs have been vulnerable to technical mal functions, malicious human activities and natural disasters as well as new forms of cyber attacks and terror.¹²¹ Actually vulnerability means a weakness in a system that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system. Cyber attacks and terror against CIIs are likely to be committed through the vulnerabilities. To protect CIIs from unintentional distortion, malfunction and shutdown

¹¹⁶ Article 16-2 para.4 of the Presidential Decree.

¹¹⁷ Article 8, para.3. of the Act.

¹¹⁸ Article 8, para.5. of the Act.

¹¹⁹ Article 8, para.6. of the Act.

¹²⁰ Hong, Jong-hyun and Cho, Young-hyuk, A Study on the Improvement of the CIIP Act, Korea Legislation Research Institute(2014. 9), 1, p.65.

¹²¹ Steven M. Bellovin. Matt Blaze. Sandy Clark and Susan Landau, Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, Privacy Legal Scholars Conference(June 2013), 1, 24(available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312107)

as a result from the cyber attacks or terror, it is urgently needed to identify vulnerabilities.

In Korea, according to CIIP Act, a MA shall analyze and evaluate the vulnerabilities of CIIs under its control on a regular basis.¹²² When an information infrastructure or a facility has been newly designated as a CII, MA, which has operated the CII, shall analyze and evaluate initially the vulnerabilities within 6 months after the designation.¹²³ If MA does not perform the analysis and evaluation within that period with a reasonable reason, MA, with a permission from CAA, shall perform the analysis and evaluation within 9 months after the designation. After initial analysis and evaluation were performed, MA shall do these with every year period. However, when there would be a critical change in the CII or MA made a decision to perform the analysis and evaluation, MA shall have these without waiting one year.¹²⁴ The MA may ask the NSRI, KISA, Information Sharing and Analysis Centers, specific consulting companies to analyze and evaluate vulnerabilities of CII under its control.¹²⁵ MSIP shall develop and establish guidelines concerning the analysis and evaluation of vulnerabilities in consultation with CAA and NCSC, and provide the guideline to the relevant CAA.¹²⁶

3.3.1.2 Measures and process

In case of performing the analysis and evaluation of vulnerabilities, MA shall establish a task force.¹²⁷ To assure objectiveness and effectiveness in analysis and assessment, the task force shall be composed of managing and operating staffs of the CII and information security experts,¹²⁸ but the chief of task force shall be the CISO of the MA. The task force shall establish a "plan for analysis and evaluation of vulnerabilities" including performance method of the analysis and evaluation of vulnerabilities, review items, process, period and budgets according to the above guideline, and perform the analysis and evaluation of vulnerabilities after reporting the plan to head of MA. The T/F shall define areas and categories of the analysis and evaluation of vulnerabilities, after looking at the composition and business operation of CII. In doing this, the T/F shall divide and select detailed infrastructures and facilities in the CII, such as physical assets, software, data, personal assets, and virtual assets. Then T/F shall identify composition map and items of the CII, and develop priorities

¹²² Article 9. para.1. of the Act.

¹²³ Article 17. para.1 of the Presidential Decree.

¹²⁴ Article 17. para.2 of the Presidential Decree.

¹²⁵ Article 9. para.3. of the Act.; Article 12 of Presidential Decree on the Protection of Information and Communication Infrastructure

¹²⁶ Article 9. para.4. of the Act.

¹²⁷ Article 9 para.2. of the Act.

¹²⁸ Article 18. para.1 of the Presidential Decree.

among them based on their importance and valuation in the CII. T/F shall also identify risks and threats which have actually happened or any possibility to happen. T/F shall analyze each risks and threats' cause and frequency, and effects when the intrusion or cyber incidents arise. The T/F shall identify risk points and vulnerabilities, and shall develop vulnerabilities review list. The T/F shall also assure and analyze that vulnerability should exist or what is the degree of each vulnerability. T/F shall detect the selected vulnerabilities using 'vulnerability detect tool' retained by MA or developed by information security assistant organizations, KISA, ISACs, specific consulting companies and NSRI.¹²⁹ In addition to use the tool, the T/F shall analyze vulnerabilities in personal, physical and managerial security structures of the MA. T/F shall review the existed Protection Measures established by MA should be appropriate and effective. T/F shall evaluate relation between risks and vulnerabilities, possibility of cyber attacks and intrusion incidents, effectiveness against MA when cyber attacks and intrusion incidents arise, protection measures to be newly needed or reinforced, economic efficiency and correlation with the existed Protection Measures. MA may permit information security assistant organizations to perform the analysis and evaluation of vulnerabilities.¹³⁰ In this case, MA may not establish the task force.¹³¹ Based on the analysis and evaluation of vulnerabilities, performed by the T/F or the information security assistant organization, MA shall develop and establish most effective protection measure, and specifically enforce and realize it.

3.3.2 Protection Measures

Considering the results from the analysis and evaluation of vulnerabilities, the MA shall establish and implement protection measures, including physical and technological measures to protect the CII.¹³² Protection measures established and developed by MA shall be submitted annually to CAA until at the end of August.¹³³ When the MA establishes the measures, it shall submit details of such measures to a CAA which supervises the agency.¹³⁴ Protection Measures shall be established by MA with its own decision based on the results from the analysis and evaluation of vulnerabilities. The measures shall be the fundamental and valuable materials necessary for establishing Protection Plans, developed by CAAs. Because Protection measures shall include technical measures and physical protection measures, not only virtual but also physical assets and facilities can be designated to CII.

¹²⁹ Article 12. of the Presidential Decree.

¹³⁰ Article 9 para.3. of the Act.; Article 12, Article 18. para 2. and 3 of the Presidential Decree.

¹³¹ Article 9 para.3. of the Act.

¹³² Article 5 para.1. of the Act.

¹³³ Article 8. of the Presidential Decree.

¹³⁴ Article 5 para.2. of the Act.

3.3.3 Reviewing Protection Measures

Although the CIIP Act describes protection measures established by MA with its own decision, the Act has not any provisions related to inspect or review the performance or enforcement of the measures. This could lead the protection measures to be practically meanness. To solve these problem, Korean government amended the Act in 2007 introducing a provision under which NCSC, MSIP and MND may review whether a MA properly implements measures to protect CII or not.¹³⁵ They may notify the result of reviewing protection measures to relevant CAA.¹³⁶ They may request the relevant CAA to submit data, including details of measures to protect CII submitted by a MA, when it is necessary for reviewing.¹³⁷ The NCSC, MSIP and MND are in charge of reviewing protection measures implemented by MAs. MAs which belong to public and governmental sector shall be reviewed by NCSC, MAs in private sector shall be reviewed by MSIP, and MAs in military sector shall be reviewed by MND.¹³⁸

When NCSC, MSIP and MND start to the reviewing, they shall consult in advance with related CAA on the procedures of reviewing, and make a notice to MA about the reviewing procedure.¹³⁹ They also ask assistance for information security assistant organizations when it is necessary for reviewing the measures.¹⁴⁰ Detailed guidelines for the reviewing shall be defined by the consult between NCSC and MISP. NCSC, MISP and MND shall make a report on the result of reviewing to the Committee.¹⁴¹ NCSC, MISP and MND shall recommend for MA to have improvements on its protection measures, which is likely to be necessary for complementary measures.¹⁴² NCSC and MISP shall reflect the result of reviewing to the guidelines for next year's protection measures and protection plans.¹⁴³ NCSC and MISP shall share the results with each other to make efficient assistances for CIIP.¹⁴⁴

3.3.4 Protection Plans

A relevant CAA shall establish and implement plans for protecting CII within its authority by integrating and coordinating the measures submitted by the MAs under its supervision.¹⁴⁵ It shall submit details on outcomes of implementing plans for protecting CII of the previous year and plans for the following year to the Committee for its

¹³⁵ Article 5-2 para.1. of the Act.; Article 9-2. para 1. of the Presidential Decree.

¹³⁶ Article 5-2 para.3. of the Act.

¹³⁷ Article 5-2 para.2. of the Act.

¹³⁸ Article 9-2. para 2. of the Presidential Decree.

¹³⁹ Article 9-2. para 3. of the Presidential Decree.

¹⁴⁰ Article 9-2. para 4. of the Presidential Decree.

¹⁴¹ Article 9-3. para 1. of the Presidential Decree.

¹⁴² Article 9-3. para 2. of the Presidential Decree.

¹⁴³ Article 9-3. para 3. of the Presidential Decree.

¹⁴⁴ Article 9-3. para 4. of the Presidential Decree.

¹⁴⁵ Article 6 para.1. of the Act.

deliberation.¹⁴⁶ Protection plans shall include i) matters concerning the analysis and the evaluation of vulnerabilities of CII; ii) matters concerning prevention against intrusion incidents against CII and measures for the resilience thereof; iii) other necessary matters concerning the protection of CII.¹⁴⁷

3.4 Responding Cyber Incidents

3.4.1 Notification

A MA shall, when it recognizes that the occurrence of intrusion incidents lead to the disturbance, paralysis or destruction of CII under its control, notify relevant administrative authorities and law enforcement authorities of such facts. In these cases, the authorities shall take necessary measures to prevent the spread of damage caused by intrusion incidents and respond urgently to such incidents.¹⁴⁸ The Government may provide governmental budget support, including costs incurred in recovering damage, to a MA that has contributed to preventing the spread of damage by notifying intrusion incidents.¹⁴⁹

3.4.2 Resilience Measures

A MA shall take necessary measures to make resilience and protect CII in a swift manner when intrusion incidents occur.¹⁵⁰ It may request a relevant CAA to provide assistance when it is necessary for taking measures for resilience and protection.¹⁵¹ However, these assistances, shall not apply to cases for technical assistance for protection of specific CIIs.¹⁵² The CAA provides necessary assistance for the resilience from damage, such as technological assistance, and takes appropriate measures to prevent the spread of damage.¹⁵³

3.4.3 Technical Assistance

MAs may also request technical assistance, if it is necessary, to the NCSC, MSIP or specialized institutions prescribed by Presidential Decree.¹⁵⁴ They may also ask a

¹⁴⁶ Article 6 para.2. of the Act.

¹⁴⁷ Article 6 para.3. of the Act.

¹⁴⁸ Article 13 para.1. of the Act.

¹⁴⁹ Article 13 para.2. of the Act.

¹⁵⁰ Article 14 para.1. of the Act.

¹⁵¹ Article 14 para.2. of the Act.

¹⁵² Id.

¹⁵³ Article 14 para.3. of the Act.

¹⁵⁴ Article 7 para.1. of the Act.

technical assistant when they would have an order from the Committee to review their CIIs because the CIIs would be likely to cause harm to national security or the economy and the society as a whole.¹⁵⁵ Technological assistances shall be i) formulation of measures to protect CII; ii) prevention of intrusion incidents against CII and the resilience thereof; iii) compliance with an order or recommendation for specific protection measures.¹⁵⁶ When a MA has a specific CII which would significantly influence on national security, it does not request for technological assistance to other institutions without asking for NCSC to have the first assistance.¹⁵⁷ A specific CII shall be one of the i) critical transportation facilities, such as roads, railroads, subways, airports and harbors; ii) facilities for water resources and energy, including electricity, gas and oil; iii) relay broadcast facilities and the national command control communication network; iv) research facilities of government-funded research institutes related to nuclear energy, the national defense and science, or advanced defense industry.¹⁵⁸ However, NCSC may provide technical assistance without any request from the MA, in consultation with the relevant CAAs, in cases where a substantial and imminent threat to national security exists and it is impossible to recover from damage if it waits for a MA's request.¹⁵⁹ However, NCSC shall not provide a technological assistance to any information infrastructure which has personal information.¹⁶⁰

3.5 Recommendations to amend the Act based on Risk Allocation¹⁶¹

Risks shall be allocated to a person, an institute or an organization which would have a power to control them. Cyber risks including cyber attacks, cyber threats and cyber crimes shall not be assigned to a person, institute an institute or an organization because cyber space shall not be controlled. Cyber security, responding and making measures, standards and policies against cyber risks, shall be regarded as public good and under market failures. A person, an institute or an organization will not be willing to take actions against cyber risks. Therefore, cyber risks shall be allocated to a state.

In Korea, to protect critical information infrastructures from cyber risks, “Critical Information Infrastructure Protection Act” has been enacted since 2001. According to the Act, cyber risks on critical information infrastructures shall be allocated to the Management Agencies, some of which are from public parts but others are form private

¹⁵⁵ Id.

¹⁵⁶ Id.

¹⁵⁷ Article 7 para.2. of the Act.

¹⁵⁸ Id.

¹⁵⁹ Id.

¹⁶⁰ Article 7 para.3. of the Act.

¹⁶¹ This part shall be come from the abstract of my article, IL SEOK(LUKE), OH, Recommendations on Reforming Critical Information Infrastructure Protection Act of Korea with a View from Risk Allocation, Ewha Law Journal, vol.19, no.1(2014. 9), 293, 326-327.

sectors. However, cyber risks shall be distributed to a state, under the principle of the risk allocation.

In considering the principle, the Act shall describe duties of a state in order to support the Management Agencies especially from the private parts. Article 25 of the Act depicts that a state shall support the Management Agencies by providing equipment, technical assistance and other supports to protect critical information infrastructures. This article shall not illustrate any detailed procedures and programs. Therefore, the Management Agencies shall not have any actions or claims against a state to enforce the duties. Therefore we recommend amending the title of this article to “governmental budget support to the Management Agencies” and insert clauses with which state shall provide “government subsidies” and “loans” directly to the Agencies. Furthermore, we recommend establishing Mutual Benefit Association of the Agencies to support each other.

The Management Agencies have a right to require ‘technical assistance’ to authorities of a state, such as ‘MSIP’, ‘NCSC’ and other institutions, when they suffer from cyber risks and prepare to establish Responding Plan or taken ‘vulnerability analysis and assessment’ according to the article 7 of the Act. However, the NCSC, the best expert technical authority on cyber security in Korean government, shall be excluded on technical assistance when a required Management Agency has a critical information infrastructure including personal information. Because all of the Management Agencies’ critical information infrastructures contain personal information, NCSC shall not aid ‘technical assistance’ even if it has a technical priority on this field.

Therefore, we recommend to amend the article 7, allowing NCSC to make technical assistance. Additionally, we recommend a new clause to the article 7-2 which mandates a duty for NCSC to maintain and protect personal information comprised in the critical information infrastructures. Under the article 7-2, we recommend describing other clauses that National Assembly shall control the technical assistance activities made by NCSC, to defend personal information.

4. Conclusion: Compromising Nuclear Protection and Prevention Act and CIIP Act

When computer and network systems in nuclear power plants should be designated as critical information infrastructure, they shall be governed not only Nuclear Protection and Prevention Act but also CIIP Act. In practice, systems designated as CII in nuclear power plants are intra network which is separated from control systems. Because control systems in nuclear power plants are actually isolated from intra network and internet, and they have their own unique features, control systems shall be secured more specific ways following Nuclear Protection and Prevention Act such as

supervised by specific authority, NSSC, specializing in atomic energy and nuclear related matters. Although there is no explicit provision, Nuclear Protection and Prevention Act shall be seemed to preempt CIIP Act in securing control systems at nuclear power plants.

However in the position of the man or women who is in charge of system security at nuclear power plants, he/she shall make double reports and documentations following the security structure regulated in the two Acts. Although the intra network and control systems are different, the supervising authorities shall usually want to check the two altogether, because the two are connected and make interactions. Therefore he or she may make a report to NSSC, National Cyber Security Center. Even in case that General Audit Authority may request reports and shall take audit in cyber security performed by nuclear power plants, he or she shall make reports and documents. This has caused a lot of burden and inefficiency for the man or woman, and for Korean society.

To resolve these duplications, we recommend CIIP Act should be amended to have a specific provision describing that nuclear power plants shall be governed and secured from cyber attacks according to the Nuclear Protection and Prevention Act. However preventing and responding cyber attack for nuclear power plants shall be compromised with nationwide policies and standards. Therefore CIIP Act shall be amended to make a process that Chairman of the NSSC shall make a reports on their activities related to cyber security for nuclear power plants by periodically. Along with the amendment, the Presidential Decree of CIIP Act shall be amended that the Chairman of the NSSC shall be a member of the Committee for Critical Information Infrastructure Protection.

In Korea governmental agencies, public corporations and institutes funded by government, including MAs except from private side, shall be under Institutional Audit. That is to say these institutions are annually under governmental audit. According to the results, the institutions budget and agent members shall be increased or decreased. After government audit and supervising have performed against the institutions including MAs, especially against public corporations operating public utilities, government shall publish and announce the ranking and grade of the audit result. Cyber security has been included as an important item of the audit but its portion is very low, compared with other items. Therefore raising on cyber security portions in institution audit would increase cyber security activities and initiatives in governmental institutions especially MAs operating public utilities including nuclear power plants.

THE FUTURE OF NUCLEAR ENERGY SECURITY

Prof. Dr. Mesut Hakkı CAŞIN

ABSTRACT

Nuclear energy has become an inseparable component in meeting global energy demand. Especially for the emerging and rapidly growing economies, it is not possible to only rely on fossil fuels (oil, natural gas, coal, etc.) thus nuclear energy seems as an important option in diversifying their energy resources. In such context, nuclear safety and security became a prominent topic which requires building effective partnerships and collaboration supported by a broad range of states and international actors. While the main framework and basic guideline for ensuring security of Nuclear Power Plants, the threats to nuclear security is getting more complex in global scale and requires more comprehensive actions. In that regard, this paper aims to develop a comprehensive perspective regarding the future of nuclear energy. Also it makes a general assessment for security dimension of nuclear energy and consider possible developments in the medium- long term scenarios and recommendations for ensuring nuclear power plant security.

Key Words: Nuclear, Energy Security, Safety, Non-Proliferation, IAEA

"If one imagines a world of tens of nations with nuclear weapons and major powers trying to balance their own deterrent equations, plus the deterrent equations of the subsystems, deterrence calculation would become impossibly complicated. To assume that, in such a world, nuclear catastrophe could be avoided would be unrealistic."

Former U.S. Secretary of State Henry KISSINGER¹⁶²

¹⁶² "Nuclear Proliferation, Risk and Responsibility", *The Trilateral Commission*, 2006, <http://trilateral.org/download/doc/nuclear.pdf>, (Accessed on 29.08.2015).

Introduction

Energy is essential for economic growth. Although the link between growth and energy use has become weaker, world's demand for energy is increasing rapidly, leading to greater competition for finite natural resources.¹⁶³ There are several economic, political, technical, institutional and geopolitical challenges facing an expanded nuclear energy industry in the 21st century. The first reason of it is the critical imbalance between the supply and demand in global energy sectors. Secondly, perhaps most importantly, the world's population will continue to grow for several decades at least. Energy demand is likely to increase even faster, and the proportion supplied by electricity will also grow faster. The key question is how we generate that electricity. Today, 68% comes from fossil fuels (41% coal, 21% gas, and 5.5% oil), 13.4% from nuclear fission, and 19% from hydro and other renewable sources worldwide. There is no prospect that we can do without any of these (though oil has a more vital role in other applications). Can nuclear energy respond to energy demand? If yes, how can we secure its implementation? Today, the world produces as much electricity from nuclear energy as it did from all sources combined in the early years of nuclear power. Civil nuclear power can now boast over 16,000 reactor years of experience and meets almost 11.5% of global electricity needs, from reactors in 31 countries. In fact, through regional grids, a much higher number of countries depend on nuclear-generated power.¹⁶⁴ Two factors helped creating this so-called "nuclear renaissance"¹⁶⁵ – emerging-market energy demand and climate change. Many countries with growing economies and middle classes are looking for ways to access reliable and diverse electricity production. With fossil fuel use increasingly less attractive because of climate change, nuclear energy –which has a very small carbon footprint– has gained more attention.¹⁶⁶ Energy security nowadays is taken to include the provision of available, affordable, reliable, efficient, environmental-friendly, properly governed and socially acceptable energy services.¹⁶⁷

¹⁶³ Columba Peoples, "New nuclear, New Security? Framing Security in the Policy Case for New Nuclear Power in the United Kingdom", *Security Dialogue*, Vol. 45, No: 2, 2014, p. 156–173.

¹⁶⁴ Nuclear technology uses the energy released by splitting the atoms of certain elements. It was first developed in the 1940's, and during the Second World War to 1945 research initially focused on producing bombs by splitting the atoms of particular isotopes of either uranium or plutonium. In the 1950's attention turned to the peaceful purposes of nuclear fission, notably for power generation. "Nuclear Power in the World Today", World Nuclear Association, Updated February 2015, <http://www.world-nuclear.org/info/Current-and-Future-Generation/Nuclear-Power-in-the-World-Today/>, (Accessed on 29.08.2015).

¹⁶⁵ The nuclear energy Renaissance is being spurred by growing electricity demand, concerns about security supply of energy and climate change.

¹⁶⁶ Toni Johnson, "Nuclear Power Safety Concerns", *Council on Foreign Relations*, 23 September 2013, <http://www.cfr.org/world/nuclear-power-safety-concerns/p10534>.

¹⁶⁷ Martin J. Pasqualettia, Benjamin K. Sovacool, "The Importance of Scale to Energy Security", *Journal of Integrative Environmental Sciences*, 2012, Vol.9, No: 3, p.167-180.

Inside of the theoretical perspective, the nuclear policy, like every policy issue, has a culture. There is an ongoing discourse that evolves and changes over time, providing interpretation and meaning for relevant events. Framing of the case for nuclear power stations and associated infrastructure in security terms is crucial in this respect. Considering that Turkey aims to use nuclear energy, we aim to discuss the concept of security, which basically plays a key role in the articulation of the policy on nuclear power.

Nuclear Energy Security and Future Concerns

Energy is the rapid locomotive of high technology, sustainable development, and a part of our daily life and society. For governments, providing sufficient capacity of energy resources helps create wealth and improve living standards for individuals and countries. Demand for electricity in emerging economies is growing very strongly – between 5% and 6% each year on average, compared to 1% or less in developed economies– and will continue to rise in the decades ahead. Moreover, many of those countries have goals to improve energy security and avoid emissions of greenhouse gases and other air pollutants. It is impossible to rely solely on natural gas or sources of renewable energy to meet this demand. Nor is it possible to rely exclusively on coal, the most carbon-intensive fossil fuel.¹⁶⁸ Growing demand for electricity because of the rapidly increasing population, urbanization and industrialization has also led the countries to look for nuclear energy options in the long run. A look into the trends in energy consumption in the region shows that the demand for nuclear energy is growing. We can say that nuclear power could help with energy diversification by providing countries with an alternate form of electricity production.¹⁶⁹ However, following the events in Ukraine in early 2014, which raised the possibility of disruptions to gas supplies as occurred in 2006 and 2009, policy proposals have focused on improving the security of energy supply, emphasizing the need to develop energy resources within the EU in a sustainable way. Such an approach would seem to enhance the prospects for nuclear power as part of an energy mix –since electricity from nuclear power plants constitutes a reliable, emission-free base-load electricity supply.¹⁷⁰

¹⁶⁸ Armen Sarkissian, Fatih Birol, “Can Nuclear Energy Fuel our Future?”, *World Economic Forum Agenda*, 10 November 2014, <https://agenda.weforum.org/2014/11/can-nuclear-energy-fuel-our-future/>.

¹⁶⁹ Matthew Fuhrmann, “Splitting Atoms: Why Do Countries Build Nuclear Power Plants?”, *International Interactions: Empirical and Theoretical Research in International Relations*, Vol.38, No: 1, 2012, https://www.gwu.edu/~igis/assets/docs/Fuhrmann_Paper.pdf, pp.29-57.

¹⁷⁰ A number of EU member states now seem to be advancing plans to keep nuclear power in their energy mix. British plans to develop nuclear power are probably the most ambitious in Europe, with proposals for up to 11 new reactors by the mid-2020s. Other member states – including Bulgaria, Finland, France, Hungary, Lithuania, Poland, Romania and Slovakia– are reviving projects that were put on ice, building nuclear reactors or moving forward with plans to do so. Vitaly Fedchenko and Ian Anthony: “Nuclear Power and the European Energy Security Strategy”, SIPRI, June 2015,

Will a nuclear renaissance help address the security threats that the states will likely face in the future? To answer this question, several dimensions of energy security should be analyzed.

The greatest potential threat to energy security may be high dependence on energy imports from other countries. Former British Prime Minister Tony Blair asserted in 2006 that “energy security will be almost as important as defense.”¹⁷¹ Also in the same year, US President Barack Obama suggested that energy security should be “one of the great American projects of the 21st century.”¹⁷² Nuclear energy security issues are important for the entire world. Their effective security and safety management requires the partnership and collaboration of a broad range of states and international actors. On the other hand, the nature of emerging threats to energy security is getting more complex at the global scale, and thus it requires international cooperation and assistance, however not only states but also international organizations and energy companies should be a party to this collaboration. Nonetheless, considering the negative trans-boundary effects of nuclear accidents, developing safety and security policies for nuclear power have a priority for the international community. Nuclear security deals with the physical protection and control of nuclear materials.

Nuclear Plant Safety Features

What are some key concepts within the nuclear safety and security subject?

Nuclear safety and security have a common purpose –*protecting people, society and the environment*. In both cases, such protection is achieved by preventing a large release of *radioactive material*.¹⁷³ Nuclear security is defined as the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities. *Nuclear security* is fundamental in the management of *nuclear technologies* and in applications where *nuclear or other radioactive material* is used or transported. States have responded to this risk by engaging in a collective

<http://www.sipri.org/media/newsletter/essay/fedchenko-anthony-june-14>, (Accessed on 30.08.2015).

¹⁷¹ Malcolm Wicks, “Energy Security is not a Luxury but a Necessity in a Dangerous World”, *The Telegraph*, 5 April 2010, <http://www.telegraph.co.uk/finance/comment/7556841/Energy-security-is-not-a-luxury-but-a-necessity-in-a-dangerous-world.html>, (Accessed on 30.08.2015).

¹⁷² “Energy Security is National Security - Complete Text TOPIC: Oil & Alternative Fuels, February 28, 2006 Energy Security is National Security, Remarks of Senator Barack Obama Governor’s Ethanol Coalition Washington”, <http://obamaspeeches.com/054-Energy-Security-is-National-Security-Governors-Ethanol-Coalition-Obama-Speech.htm>, (Accessed on 30.08.2015).

¹⁷³ Nuclear safety: “The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards.” Nuclear security: “The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.” See, IAEA Safety Glossary.

commitment to strengthen the protection and control of such material and to respond effectively to nuclear security events.¹⁷⁴ The operation of nuclear power plants requires careful attention to safety, security and safeguards. Safety, of course, is aimed at *preventing accidents*; security is aimed at preventing intentional acts that might *harm the nuclear power plant* or result in the *theft of nuclear materials*; and safeguards are aimed at preventing the diversion of *nuclear materials for nuclear weapons purposes*.¹⁷⁵ Although these activities have a different focus, they overlap with each other. Actions that are taken to further one activity can have implications for the others. Achieving both safety and security in a nuclear power plant requires *good communication among individuals* with different objectives and backgrounds. Management needs to promote both a *safety and a security culture* that serves to ensure that both objectives receive appropriate attention.¹⁷⁶

To be guarded against natural accidents, terrorist sabotage, and possible combinations of these two classes of events, nuclear plant operators and regulators should consider a combined approach called nuclear safety-security. Nuclear facilities could improve safety-security in technical ways, including more secure emergency electrical supplies, better security for control rooms, and, at new plants, reactor containment structures built to survive attacks by terrorist-flown airplanes. At the institutional level, regulators could strengthen the safety-security interface by ensuring that from beginning to end, from design to dismantlement, safety and security are considered.

Nuclear power stations are highly regulated in all security and safety matters. Nuclear safety covers the whole life cycle of a nuclear installation. It includes: nuclear reactor safety, nuclear fuel safety, nuclear waste management and decommissioning, and emergency preparedness. Each nuclear plant design features reliable and diverse safety systems and strong physical barriers to prevent incidents that could pose a

¹⁷⁴ "Computer Security at Nuclear Facilities", IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual, International Atomic Energy Agency, Vienna, 2011, http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf, (Accessed on 30.08.2015).

¹⁷⁵ Nuclear power plants pose two basic security concerns. First, all nuclear reactors both use and produce radioactive elements (e.g., uranium and plutonium) that can be used to build nuclear weapons. Second, all reactors and nuclear-waste storage facilities contain large amounts of radioactive material. This material might be stolen for later use as a terrorist weapon (e.g., by being combined with conventional explosives to form a radiological dispersal weapon, also termed a "dirty bomb") or, in the case of concentrated fuel, to build nuclear weapons. Alternatively, radioactivity might be released directly to the environment by sabotaging safety systems or blowing up a facility with missiles, planted charges, or hijacked jet aircraft. Thus, nuclear facilities on a nation's own territory threaten its security as a target of enemy action, while nuclear facilities on an enemy's territory threaten security as a possible source of nuclear weapons.

¹⁷⁶ "The Interface Between Safety and Security at Nuclear Power Plants", A Report by the International Nuclear Safety Group, INSAG-24, International Atomic Energy Agency, Vienna, 2010, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1472_web.pdf, (Accessed on 30.08.2015).

threat to public health and safety. The same features that safeguard the public and the environment from a radiation release also defend the reactor from outside interference.

The IAEA seeks to build and strengthen the international safety and security regime through the development of advisory international standards, codes and guides. In the safety area, these cover nuclear installations, radioactive sources, radioactive materials in transport and radioactive waste. In 2006, the Fundamental Safety Principles were adopted by the IAEA. IAEA's safety standards are applied to enhance nuclear and radiation safety in power generation, medicine, industry, agriculture, research and education.¹⁷⁷ The 2010 Washington summit focused exclusively on preventing nuclear terrorism –that aims to stop terrorists acquiring enough fissile material to make a nuclear bomb. US President Barack Obama won support for his ambitious goal of securing all vulnerable fissile material within four years. The meeting provided the necessary high-level political involvement to overcome bureaucratic hurdles to shoring up the nuclear-security framework. This topic also has been an impact on the agenda for the Seoul 2012 Nuclear Security Summit (NSS). Seoul 2012 meeting would address the threat of radiological terrorism, and in the light of the Japanese accident, nuclear safety will also be added to its remit. Radiological terrorism includes attacks that could lead to a release of radiation, such as an attack on a nuclear facility or acquisition of radioactive material to build a 'dirty bomb'. Firstly, the summit would raise public understanding of the entire set of safety and security issues, and thus lend legitimacy to nuclear-security efforts.¹⁷⁸ At the 2012 IAEA General

¹⁷⁷ The ten principles are:

1. The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks.
2. An effective legal and governmental framework for safety, including an independent regulatory body, must be established and sustained.
3. Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks.
4. Facilities and activities that give rise to radiation risks must yield an overall benefit.
5. Protection must be optimized to provide the highest level of safety that can reasonably be achieved.
6. Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.
7. People and the environment, present and future, must be protected against radiation risks.
8. All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.
9. Arrangements must be made for emergency preparation and response to nuclear or radiation incidents.
10. Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.

The IAEA must apply these principles in its own operations. However, these principles are not binding on member states as they are non-mandatory recommendations only. See IAEA Safety Standards for protecting people and the environment "Fundamental Safety Principles, Safety Fundamentals No SF-1", http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf, (Accessed on 30.08.2015).

¹⁷⁸ A. Nicoll, "Nuclear Security after Fukushima", *Strategic Comments*, Vol. 17, No: 6, 2011, p. 1-3, <https://www.iiss.org/en/publications/strategic%20comments/sections/2011-a174/nuclear-security-after-fukushima-c823>, (Accessed on 30.08.2015).

Conference, Director General Yukiya Amano said he expected “a steady rise in the number of nuclear power plants in the world in the next 20 years.” His low case for 2030 projected a nuclear power capacity increase of about 25 percent, and his high case projected a doubling of current capacity.¹⁷⁹

Nuclear power plants have also been discussed as potential terrorist targets –as have other infrastructures such as gas pipelines and LNG terminals. Such risks need to be taken seriously. The potential consequences of an attack on a nuclear plant are more serious than attacks on other forms of infrastructure. In classic cyber security, threat(s) are some articulation of a specific challenge to confidentiality, integrity, and availability (C-I-A).¹⁸⁰ First of all, cyber security shall involve operational personnel to top management executives. National states have different cyber security maturity levels. The states need to understand our dependency on computer systems. Also, it's important that we need to develop a better understanding on the latest attacking vectors and capability of bad guys. However, we should not ignore changing dynamics in attacking vectors.¹⁸¹ The insider threat is an entity with authorized access that has the potential to harm an information or control system through destruction, disclosure, modification of data, and/or denial of service.¹⁸²

Nuclear Energy Sector in Terms of Environmental Security

Why do Many Countries Build Nuclear Power Plants?

We think that the first reason is the increasing global demand for energy, specifically electricity; the quest for energy security or diversity; and the need to control climate

¹⁷⁹ IAEA Director General Yukiya Amano, “Introductory Statement to Board of Governors,” June 08, 2015, Vienna, <https://www.iaea.org/newscenter/statements/introductory-statement-board-governors-63>, (Accessed on 30.08.2015). At this gathering, Director General Amano noted that “it remains clear from the Agency’s latest projections that nuclear power will remain an important option for many countries, despite the Fukushima Daiichi accident. Our new low projection is for nuclear power capacity to grow by nearly 25 percent from current levels to 456 gigawatts by 2030. Our high projection is 740 gigawatts, which is twice current levels.”

¹⁸⁰ P. Craig, S. Godwin, “Threat Awareness and Sharing: A model for Shifting Advantage to the Defender”, *International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange*, 1-5 June, 2015, Vienna, Austria, IAEA-CN-228/PS-II/079.

¹⁸¹ Defeating Cyber Attacks: Essential Factors

For persons → Recognition, judgment and action

For organizations → Detect, triage and respond

For countries → Intelligence, decision making and enforcement.

¹⁸² Tackling insider threat requires:

1. Enhancing research and development devoted to cyber security,
2. Awareness of the need for security of information systems and networks and what is necessary to enhance security,
3. Acting in a timely and cooperative manner to detect and respond to security incidents,
4. Reviewing and assessing the cyber security measures, and make appropriate, modifications to security policies, practices, measures and procedures, and reexamine mistakes,
5. Benefiting from lessons learned and best practices.

change. Secondly, using high technology, in the form of improved efficiency of existing reactors and the promise of advanced reactor design will be more secure, is also a driver. Thirdly, after the Cold War era, we faced with the changing nature of international balance of power and with political and strategic motivations that merit consideration.

With an increasingly resource-hungry planet desperate for a source of reliable, emissions-free power, the disaster of Chernobyl and the accident at Three Mile Island receding into distant memory, the idea of an expansion in atomic energy is enjoying a comeback in policy making and industry circles.¹⁸³ On the other hand, nuclear energy offers important benefits that contribute to meeting the nation's future energy needs. It helps conserve other fuels for purposes for which they are uniquely suited. It provides a competitive source of energy with costs which do not vary appreciably with location. It significantly reduces the problem of air pollution¹⁸⁴ and has other important environmental advantages. It is a positive element in our foreign trade; and it provides

¹⁸³ The vast majority of the remainder of the nuclear reactor fleet is based on the pressurized water reactor (PWR) design developed in the 1990s. Most reactors in operation today rely on a once-through, low-enriched uranium (LEU) fuel cycle. If it is to replace the outgoing reactors and meet the new generation requirements that a nuclear renaissance suggests, the industry must undergo a period of rapid and sustained construction. In the medium term, the reactor-related security implications of an expanded global nuclear power sector hinge on next-generation reactor designs. So-called 'generation III' and 'generation III+' designs build on the fundamental principles of generation II light water reactors (LWRs) are aiming to increase safety through the use of simplified reactor designs and passive safety features. Notable among the generation III designs are the Advanced Boiling Water Reactors (ABWR), collaboration between America's General Electric and Hitachi currently operational in Japan, and Mitsubishi Heavy Industries' Advanced Pressurized Water Reactors (APWR), scheduled to enter service in Japan in 2016/17. Further out, the so-called 'generation IV' set of reactor designs present a new combination of operational advances and potential security concerns. Among these is the resurrection of the fast reactor design, which underpins at least three of the six generation IV concepts shortlisted by the Generation IV International Forum (GIF), an international consortium. With their ability to use reprocessed spent fuel as an input and to 'burn-up' long-lived nuclear waste, fast reactors have long been recognized as a potential solution to extracting better efficiency from the fission process and as a means of reducing existing stockpiles of spent fuel. Large-scale enrichment plants are currently in place in France, Germany, the Netherlands, the UK, the US and Russia. Smaller scale enrichment operations are in place in Japan, China, Brazil, India and –famously– Iran. North Korea also claims that it is in the final stages of uranium enrichment, while Israel is widely believed to be in possession of enrichment capabilities. Charles Ebinger and Kevin Massy, "Security Implications of the Expansion of nuclear Energy", *South Asian Survey*, Vol. 17, No. 1, March 2010, p.1 75-189, James T. Ramey, "The Promise of Nuclear Energy", *The Annals of the American Academy of Political and Social Science* , Vol. 410, No.1, November 1973, pp. 11-23.

¹⁸⁴ Nuclear power continues to generate enthusiasm based on its potential to reduce greenhouse gas emissions. A single pound of reactor-grade uranium oxide produces as much electricity as over 16,000 pounds of coal –enough to meet the needs of the average U.S. household for more than a year. While burning 16,000 pounds of coal generates thousands of pounds of carbon dioxide, sulfur dioxide, and nitrogen oxides - nuclear power is virtually emissions-free. Lucas W. Davis, "Prospects for Nuclear Power", *The Journal of Economic Perspectives*, Vol. 26, No. 1, Winter 2012, pp. 49-66.

freedom from overreliance on foreign energy sources. Nuclear energy can be a significant component of sustainable energy systems.¹⁸⁵ Some studies have been undertaken on the environmental and sustainability aspects of nuclear power, which support this view.¹⁸⁶ In addition, nuclear power is an opaque, technologically complex, and –let's be forthright– potentially hazardous way to generate electricity. Because of these characteristics, some people will always view the technology with skepticism or suspicion and argue that the benefits are not worth the risks. In addition, in part because nuclear power presents many potential benefits, there will always be others, usually with more thorough technical expertise, who see it as an obviously elegant solution to major energy and climate constraints and whose risks are relatively small and manageable.¹⁸⁷

How Do Nuclear Accidents Influence Global Nuclear Power Development?

However, from the other side, considering the fact that four years after the Fukushima disaster¹⁸⁸ none of Japan's 48 reactors are back online and the nuclear's share of

¹⁸⁵ Marc A. Rosen and Ibrahim Dincer, "Nuclear energy as a component of sustainable energy systems", *International Journal of Low Carbon Technologies*, Vol. 2, No: 2, 2007, p. 109.

¹⁸⁶ In doctrinal framework, Rashad and Hammad have comparatively assessed the environmental and health impacts of nuclear and other electricity-generation systems. The study includes normal operations and accident scenarios, and accounts for the full energy supply chain, and the environmental impacts from the waste-management cycles are also discussed. The authors point out that nuclear power, while economically feasible and meeting 17% of global electricity demand is almost free of the air polluting gases that threaten the global climate. Nuclear power is seen to compare well with other sources for electricity generation in terms of such environmental emissions as SO₂, NO_x, CO₂, CH₄ and radioisotopes, taking into account the full fuel chains. Duffey describes the role of nuclear energy in a sustainable future, addressing social, economic and environmental concerns. Over 400 nuclear reactors operating worldwide today avoid annual emissions of nearly two billion tons of greenhouse gases (GHGs), yet they receive little recognition for the emissions avoidance in current Kyoto and other policies. See, S. M. Rashad and F. H. Hammad, "Nuclear power and the environment: Comparative Assessment of Environmental and Health Impacts of Electricity-generating Systems", *Applied Energy*, Vol. 65, 2000, pp. 211–229, R. B. Duffey, "Sustainable futures using nuclear energy", *Progress in Nuclear Energy*, 2005, Vol. 47, No. 1, Issue, 4, pp. 535–543, cited in Marc A. Rosen and Ibrahim Dincer: "Nuclear energy as a component of sustainable energy systems", *International Journal of Low Carbon Technologies*, Vol. 2, No.: 2, 2007, p. 112.

¹⁸⁷ Nathan E. Hultman, "Risk, Benefit, and Choice: Is Nuclear Power the Answer to Future Energy Constraints?", *Environmental Practice*, Volume 10, Issue 2, June 2008, p. 41.

¹⁸⁸ In the early afternoon of 11 March 2011, the most powerful earthquake ever to hit Japan struck the ocean floor approximately 70 kilometers off Japan's northeast coast. The earthquake measured 9.03 on the moment magnitude scale, and was one of the five most powerful earthquakes ever recorded since recordkeeping began in 1900. Approximately an hour after the earthquake struck, massive tidal waves –some reaching a colossal 133 feet in height– generated by the earthquake, began to make landfall along the northeast coast of the Japanese islands of Honshu and Hokkaido. The hardest hit area of coastline was in the Tohoku area of Honshu, and extended from Ibaraki prefecture in the south, to Iwate prefecture in the North; a distance of some 250 miles. In September 2012, a year and a half after the earthquake and tsunami disaster, a Japanese National Police Agency report confirmed that the event had caused 15,878 deaths; 6,126 injuries; and 2,713 people to yet

global electricity generation has fallen from 17% to 11% in the past 20 years; you might assume the industry is in terminal decline.¹⁸⁹ After the disaster of Fukushima in March 2011, some countries, especially Germany, changed their energy policy dramatically in order to end the use of nuclear fission in energy production.¹⁹⁰

Each year, the OECD's International Energy Agency (IEA) sets out the present situation and also reference and other –particularly carbon reduction– scenarios. World Energy Outlook 2014 had a special focus on nuclear power, and extends the scope of scenarios to 2040. In its New Policies scenario, installed nuclear capacity growth is 60% through 543 GWe in 2030 and to 624 GWe in 2040 out of a total of 10,700 GWe, with the increase concentrated heavily in China (46% of it), plus India, Korea and Russia (30% of it together) and the USA (16%), countered by a 10% drop in the EU. Despite this, the percentage share of nuclear power in the global power mix increases to only 12%, well below its historic peak. Low-Nuclear and so-called High-Nuclear cases give 366 and 767 GWe nuclear respectively in 2040. The low-carbon '450 Scenario' gives a cost-effective transition to limit global warming, assuming an effective international agreement in 2015, and this brings about more than doubling nuclear capacity to 862 GWe in 2040, while energy-related CO₂ emissions peak before 2020 and then decline. In this scenario, almost all new generating capacity built after 2030 needs to be low-carbon.¹⁹¹ But, there is an estimated 200 reactors, or nearly half of the global nuclear capacity, are heading for retirement over the next 25 years, according to the International Energy Agency. The nuclear energy industry wants to not only replace that lost capacity, but also to grow its market share. The next generation of nuclear technology will need to demonstrate significant improvements over these hulking 20th century beasts.¹⁹² Europe, countries that had turned their backs on the

be missing across twenty prefectures. It caused 129,225 buildings to totally collapse, with an additional 254,204 buildings 'half collapsed', and a further 691,766 buildings partially damaged. The World Bank has estimated that the overall economic cost of the disaster was \$235 billion, making it the most costly natural disaster in world history. Daniel H. Joyner: "Nuclear Power Plant Financing Post-Fukushima, and International Investment Law", *Journal of World Energy Law and Business*, Vol. 7, No. 2, 2014, p.70.

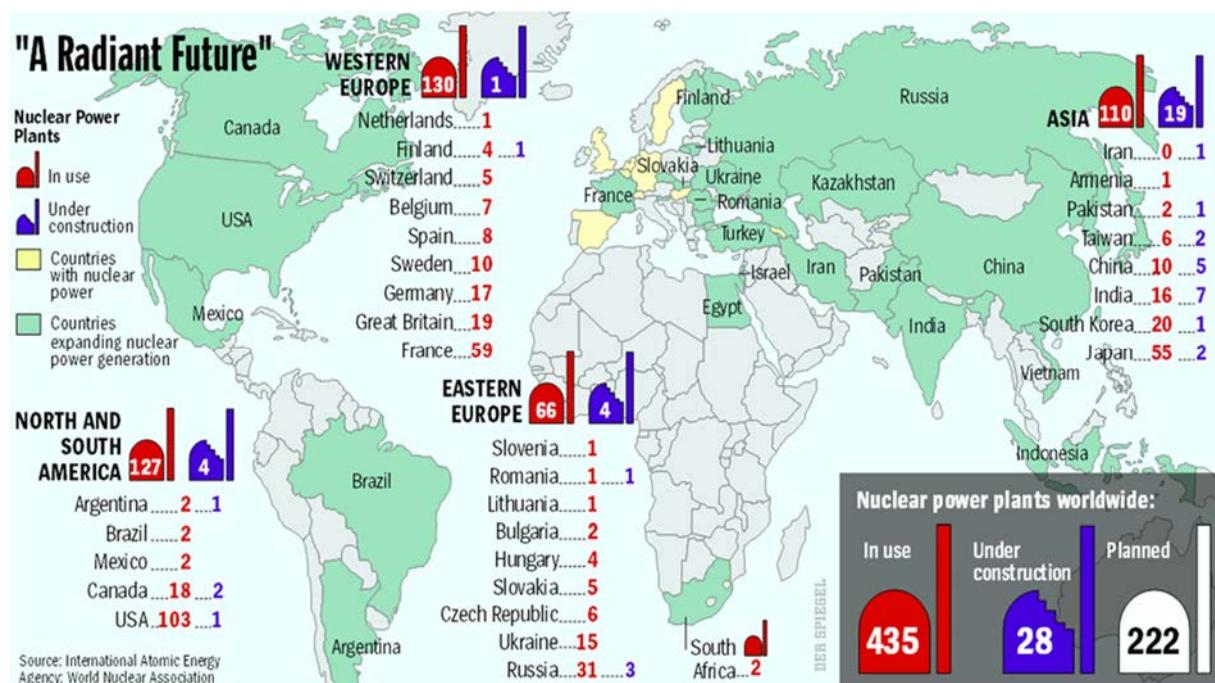
¹⁸⁹ Richard Anderson, "Nuclear power: Energy for the Future or Relic of the Past?", BBC, 27 February 2015,<http://www.bbc.com/news/business-30919045>, (Accessed on 30.08.2015).

¹⁹⁰ Gerd Winter, "The Rise and Fall of Nuclear Energy Use in Germany: Processes, Explanations and the Role of Law", *Journal of Environmental Law*, Vol.25, No: 1, 2013, p. 95.

¹⁹¹"Plans for New Reactors Worldwide", World Nuclear Association, May 2015, <http://www.world-nuclear.org/info/Current-and-Future-Generation/Plans-For-New-Reactors-Worldwide/>, (Accessed on 30.08.2015).

¹⁹² The generation of nuclear reactors constructed in the 1970s and 1980s are showing their age. In just the past week, several U.S. reactors faced some equipment problems, forcing them to shut down. The Fermi 2 nuclear power plant outside of Detroit was taken offline after a water leak on March 19. The Oyster Creek nuclear plant in New Jersey was forced to temporarily shut down due to an electrical problem. These problems are minor, to be sure, but illustrate some of the issues plaguing America's nuclear fleet, the world's largest. The oldest and –according to industry consensus– least safe nuclear reactors currently in operation are the handful of so-called 'generation I' reactors. These include the three remaining VVER-440 230 reactors (two in Russia, one in Armenia), which lack emergency core cooling systems and the British Magnox design reactors, which have no secondary

idea of nuclear power are doing an about-face: in February 2009, Italy announced that it was going to restart nuclear production after banning it in the wake of the Chernobyl disaster; the same year, the Spanish government granted an extension to its oldest civilian nuclear plant in 2009 despite having previously committed to phasing out nuclear power by 2006; and Sweden has overturned its moratorium on new nuclear power stations and has even offered to provide a nuclear waste repository for the rest of the world.¹⁹³



containment systems and incorporate components that are particularly subject to corrosion (National Academy of Science), [NAS]1995). Nick Cunningham: "A Look at the Future of Nuclear Power", *Oil Price*, 24 March 2015, <http://oilprice.com/Alternative-Energy/Nuclear-Power/A-Look-At-The-Future-Of-Nuclear-Power.html>, (Accessed on 30.08.2015).

¹⁹³ France imports half of its net primary energy, and this is a significant justification for its heavy reliance on nuclear power for electricity, since uranium is a small part of the power cost. This policy of having three quarters of its electricity from nuclear power was set in 1973 –see Figure 2. France is a world leader in nuclear fuel cycle and reactor building, and uranium is easily stockpiled. Germany imports more than half its net primary energy and in the past it has addressed this vulnerability with one third of electricity from nuclear and also major incentives for renewables. Japan imports nearly 85% of its primary energy and has framed energy policies in the light of this vulnerability. Its policy since the 1970s has been to have a balance among coal, gas and nuclear, with this changing since 2000 to increase the nuclear proportion. However, since the Fukushima accident this is being reviewed.

The UK imports less than 20% of its net primary energy, but this is set to increase with depletion of North Sea gas. Continuing a high reliance on gas would make it vulnerable to supply interruptions from Siberia and the Middle East. The USA imports almost 20% of its net primary energy today (less than in the 2007 diagram), mostly as oil and gas, and this is regarded as having a major influence on its defense budget. The advent of low-cost shale gas is helping its situation in the short term.

Energy Security, World Nuclear Association, April 2014, <http://www.world-nuclear.org/info/Economic-Aspects/Energy-Security/>, (Accessed on 30.08.2015).

Source: <http://www.superaktif.net/wp-content/uploads/2010/07/NuclearPlantsWorldMap.gif>

What Will It Take for Nuclear Power to Enter the Marketplace?

Building nuclear plants in China, as well as in some other developing economies, is relatively straightforward. For a start, they are much cheaper to construct –typically between \$10bn (£6.5bn) and \$15bn– while the state-controlled economy provides the necessary regulatory and financial support. Three hundred and seventy-three reactors with a combined installed capacity of 438 GW produce nuclear power globally. They are on average 25 years old, and less than 10 percent have come on stream since 2000. The US, France, Japan, Russia, and South Korea account for more than 80 percent of today's nuclear power production, although only Russia, Japan, and South Korea have increased its installed capacity during the past decade. The much hailed 'nuclear renaissance' is happening in Asia and Russia. China expects to bring on stream 60 GW, India 25 GW, South Korea 20 GW, and Russia 25 GW by 2020.¹⁹⁴

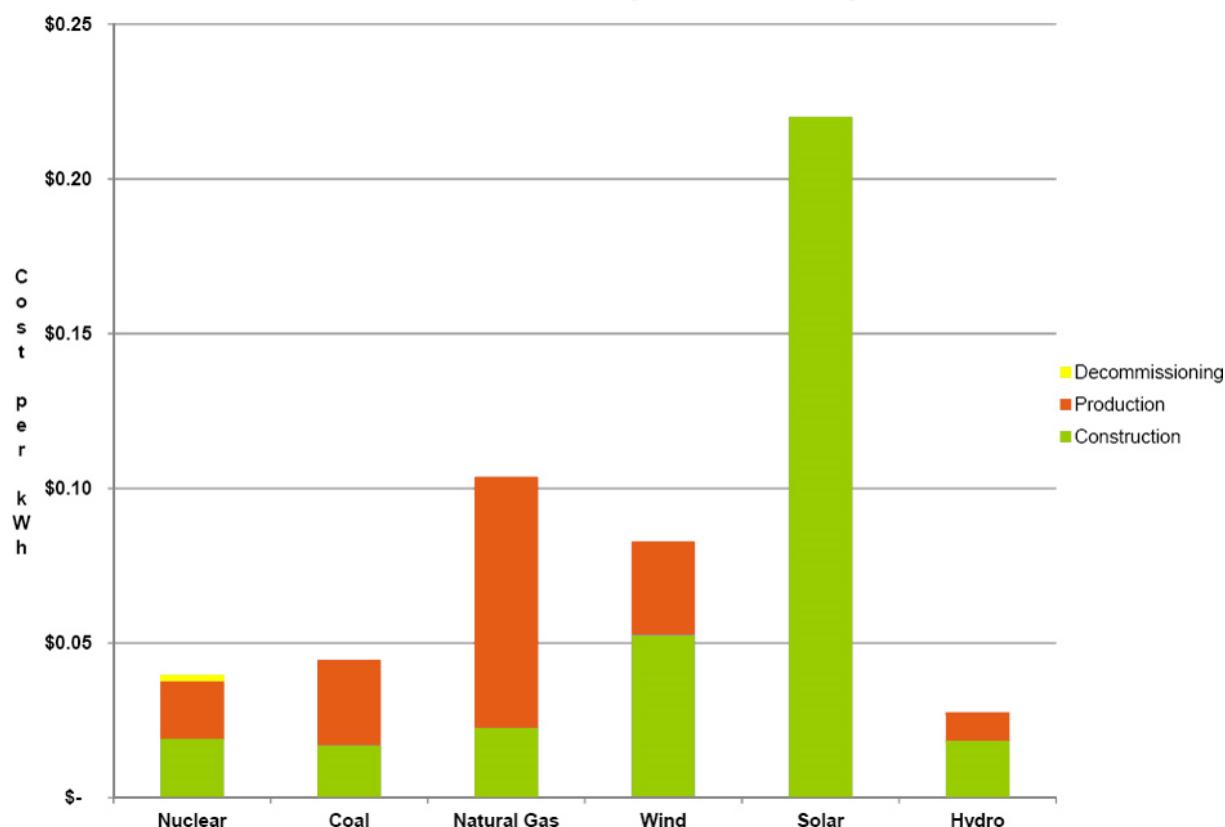
Will Costs Constitute an Important Factor for Nuclear Energy in the Future?

Once a nuclear power station has been built, it is relatively cheap to run. There is plenty of uranium in the world and, in terms of cost per unit; it is cheaper than fossil fuels. Of course a good many will never see the light of day, but these figures show clearly that the governments across the world are seeking the help of the nuclear power in order to solve some of the most pressing dilemmas they face –namely how to meet growing energy demand and increase energy security while reducing the CO₂ emissions linked

¹⁹⁴ Conventional nuclear power reactors do use a mineral fuel and demonstrably deplete the available resources of that fuel. In such a reactor, the input fuel is uranium-235 (U-235), which is part of a much larger mass of uranium –mostly U-238. This U-235 is progressively 'burned' to yield heat. But about one-third of the energy yield comes from something which is not initially loaded in: plutonium-239 (Pu-239), which behaves almost identically to U-235. Some of the U-238 turns into Pu-239 through the capture of neutron particles, which are released when the U-235 is 'burned'. So the U-235 used actually renews itself to some extent by producing Pu-239 from the otherwise waste material U-238. This process can be optimized in fast neutron reactors, which are likely to be extensively deployed in the next generation of nuclear power reactors. A fast neutron reactor can be configured to 'breed' more Pu-239 than it consumes (by way of U-235 + Pu-239), so that the system can run indefinitely. While it can produce more fuel than it uses, there does need to be a steady input of reprocessing activity to separate the fissile plutonium from the uranium and other materials discharged from the reactors. This is fairly capital-intensive but well-proven and straightforward. The used fuel from the whole process is recycled and the usable part of it increases incrementally. As well as utilizing about 60 times the amount of energy from uranium, fast neutron reactors will unlock the potential of using even more abundant thorium as a fuel (see information page on Thorium). Using a fast neutron reactor, thorium produces U-233, which is fissile. Nuclear Energy Association, Sustainable Energy, June 2013, <http://www.world-nuclear.org/info/Energy-and-Environment/Sustainable-Energy/>, (Accessed on 30.08.2015).

with global warming. Cost, capital intensity, and technological complexity make it difficult for some states to rely on nuclear energy. Nuclear power plants may be cost-competitive with coal and gas fired power plants in the long run because they have low marginal operating costs. Yet they are more expensive to build. The front end costs of power plant construction vary based on country-level factors but the average construction costs for coal, gas, and nuclear power plants are informative. A country's level of economic growth may also influence the attractiveness of nuclear power. Higher levels of growth increase the demand for energy; building nuclear power plants is one option that could increase electricity needs.¹⁹⁵

Total Cost of Electricity Production per kWh



Source: <https://conservativecritic.files.wordpress.com/2013/10/total-cost-electricity-production-per-kwh.jpg>

¹⁹⁵ Consider some data from a 2010 study produced by the International Energy Agency (IEA) on the costs of electricity production based on a sample of 190 power plants in 21 countries. The overnight construction costs of nuclear power plants ranged from \$1,600 to \$5,900 per kWe with a median value of \$4,100 per kWe. Most coal-fired power plants had overnight investment costs ranging from \$900 to \$2,800 per kWe while the same costs for gas-fired plants ranged from \$520 to \$1,800 per kWe. If we simply compare the high-end estimates for each plant type, the overnight construction costs of nuclear power plants are 111% more expensive than for coal-fired plants and 228% more expensive than for gas-fired plants.

A carbon tax is an economically efficient means of incentivizing carbon-reducing investments in electrical generation systems. Along with growing demand for electricity and a desire to mitigate climate change, there has been renewed discussion about the role of nuclear power in meeting CO₂ emission reduction targets. With the generating mixes of most electrical grids dominated by fossil fuels, economic incentives such as a carbon tax or cap-and-trade scheme will lead to a substantial increase in the cost of generation or a significant transformation to lower CO₂ emitting technologies such as hydroelectric dams, wind turbines and nuclear power plants.¹⁹⁶ How clean is clean energy? Every kind of energy is clean in its own way. According to International Energy Agency's 2010 data, typical CO₂ emissions in t/MWh for electricity generation are estimated at 0.002 for wind, 0.005 for nuclear, between 0.009 and 0.017 for solar, 0.142 for CCS from coal, and 0.777 for an ultra-supercritical coal combustion. Thus, the carbon reduction impact of wind, solar, and nuclear compared to modern coal-burning power technology is a factor of 100 and above, but only a factor of 5 for CCS. In contrast, biomass averages greenhouse gas (GHG) savings of 63–99 percent compared to coal in power generation.¹⁹⁷

Many view nuclear as a key part of the solution, and none more so than China. The country is building 27 new reactors and has plans for almost 200 more, according to the WNA. The reason is simple –demand for energy is expected to be tripled by 2050, so China needs all the power it can get.

1. Nuclear Waste Problem and Security Dimension

Spent nuclear fuel, one of the most dangerous and toxic materials known, can be reprocessed into fresh fuel or into weapons-grade materials, and generates large amounts of highly active waste.¹⁹⁸ How reliable are the cost estimates of the nuclear industry for new installations under today's more stringent safety rules? Nearly all countries struggle with permitting, plant siting, and safety regulations acceptable to the public and regulators. The nuclear waste disposal and storage issues have not been solved satisfactorily and it remains an uninsurable, public liability. Short- and long-term storage of spent nuclear fuel has been a challenge for the industry and policymakers. Spent fuel, if not disposed of properly, could contaminate water supplies or be used by terrorists to create a dirty bomb. In the short-term, spent fuel is stored in pools on-site, but they only need to stay there a few months until they are cool enough to move to dry storage (either on site or in a long-term storage facility). Still, at some plants, fuel

¹⁹⁶ G. Cornelis van Kooten, Craig Johnston, and Linda Wong, "Wind versus Nuclear Options for Generating Electricity in a Carbon-Constrained World: Strategizing in an Energy-Rich Economy", *American Journal of Agricultural Economics*, January 2013, Vol. 95, pp.505-511.

¹⁹⁷ Marianne Haug, "Clean Energy and International Oil", *Oxford Review of Economic Policy*, Volume 27, Number 1, 2011, pp. 92–116.

¹⁹⁸ Nuclear waste is generally classed into three categories, 'High Level' (HLW), intermediate (ILW) and low (LLW): A fourth category, very low (VLLW) may be listed separately or incorporated into LLW.

rods are packed in pools in numbers well above design specifications and stay in the pools long after they are ready to be moved (R&D). Fukushima revived U.S. discussion (Beacon) about plans for a long-term storage facility at Yucca Mountain in Nevada that had been scrapped. Meanwhile, advocates say utilities should be required to move spent fuel to hardened, dry-cask storage as soon as possible. Efforts to reprocess nuclear waste are expensive and come with associated environmental and security risks. Yet a growing number of countries –including Japan and Russia– have begun fuel recycling projects.¹⁹⁹

2. Legal Regime of Nuclear Energy Usage and States' Non-proliferation Responsibility

The IAEA is often referred in the international media as the UN's nuclear watchdog; a title that helps people visualize its global nuclear security role but gives an overly narrow impression of the agency's work. It has also been tasked with monitoring member state compliance with their legal obligations and with dealing with states that violate them.²⁰⁰ In 1999, the IAEA introduced a new concept for nuclear facility security, the design-basis threat, defining it as the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated. Although details of particular design-basis threats vary by country and power plant and remain confidential, the IAEA's publication released in 2011 –Nuclear Security Recommendations on Physical Protection of Nuclear Material and Facilities– provides a basic guideline.

The biggest obstacle to expand IAEA's authority is that IAEA member states are deeply divided over the agency's priorities. Many resist efforts to expand the IAEA nuclear security mandate. Whereas most Western states are keen to expand IAEA's role and authority in the 3Ss (safety, security, and safeguards), many developing states believe that the IAEA is already doing enough in those areas and that efforts to expand its role further undermine what they see as its core role: assisting states in the utilization of nuclear technology for peaceful purposes harkening back to the IAEA's original role as a promoter of nuclear power. Furthermore, some developing states also hint at deeper concerns that Western states are using the IAEA to fulfill their own security/intelligence agendas. The IAEA is the right organization to manage all the components of a strong

¹⁹⁹ Toni Johnson, "Nuclear Power Safety Concerns", *Council on Foreign Relations*, 23 September 2011, <http://www.cfr.org/world/nuclear-power-safety-concerns/p10534>, (Accessed on 29.08.2015).

²⁰⁰ We must remember that, since the 1960s, the peaceful use of nuclear energy has expanded around the world, and as the volume of nuclear materials and their international transport increased, so did concerns about the protection of nuclear materials against terrorist groups. International regulation of nuclear material, in fact, began decades ago, in programs spearheaded by the United States and the International Atomic Energy Agency (IAEA).

nuclear security infrastructure. However, the agency does not have the authority to independently evaluate states' nuclear security.²⁰¹

There is no specific international treaty requiring any level of protection for power or research reactors from terrorists. The relevant treaty, the Convention on Physical Protection of Nuclear Material, only provides protection standards to protect nuclear material from being stolen while it is in international transport. In this regard, the question of what international and legal frameworks apply in case of a cyber attack against a nuclear facility depends on several factors. Some of the international legal frameworks will be applied against the attackers.²⁰² However, legal scholars disagree over the applicability of the existing international norms, principles, and standards to cyber space activities. While some believe that the existing regulations and standards are not applicable to cyber space, there are those who believe that existing regulations are fully applicable to cyber space activities. There are also several disagreements among the scholars who believe that international regulations and standards are applicable to cyber space activities.²⁰³

I argue in this section that the cornerstone of this legal regime is the 1968 Nuclear Non-Proliferation Treaty (NPT), which codified an agreed framework of basic rights and

²⁰¹ Jack Boureston and Tanya Ogilvie-White: "Expanding the IAEA's nuclear security mandate", *Bulletin of the Atomic Scientists*, September/October 2010; vol. 66: 5, pp. 55-64.

²⁰²Council of Europe, "Convention on Cyber Crime", Budapest, November 2001,

<http://conventions.coe.int/Treaty/EN/Treaties/Htm/185.htm>, United Nations, Convention on the Physical Protection of Nuclear Material (with annexes). "Convention on the Physical Protection of Nuclear Material", U.S. Department of State Bureau of International Security and Nonproliferation, Signed at New York March 3, 1980, Entered into force February 8, 1987, <http://www.state.gov/t/isn/5079.htm>, "Nuclear Security - Measures to Protect Against Nuclear Terrorism Amendment to the Convention on the Physical Protection of Nuclear Material Report by the Director General, Board of Governors General Conference GOV/INF/2005/10-GC(49)/INF/6 Date: 6 September 2005", <https://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf>, Viktor Boulanin: "International and Legal Frameworks Addressing Cyber Attacks against Nuclear Facilities: The State of Play", CN-228 *International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange*, 1-5 June, 2015, Vienna, Austria, IAEA-CN-228/5A1/138, (Accessed on 30.08.2015).

²⁰³ These disagreements are over which part of the international law is applicable to cyber space activities (especially when it comes to the so-called cyber warfare activities).

Regardless of these general disagreements, recent developments show that the threat from cyber attacks to international security is real. The attack on Iranian nuclear facilities and the ability to cause remote damage via information and communications technology by sophisticated cyber attack; the damage cyber criminals or state-sponsored attacks could cause to national security via financial sector; and the damage that patriotic hackers' or terrorist use of a cyber space can cause via cyber space have proven unequivocally the complexity of the cyber attacks—not just from strategic-security and technical aspect, but also from a legal aspect. M. Hadji-Janev, "Evaluating the Applicability of the Existing Principles and Standards of International Law to Cyber", CN-228 *International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange*, 1-5 June, 2015, Vienna, Austria, IAEA-CN-228/5A1/187.

responsibilities of states with regard to nuclear energy.²⁰⁴ In a world of expanded nuclear energy demand, both the ideological and practical aspects of the NPT (and other international non-proliferation regimes) face new challenges. Basically, in global dimension perspective, as the use of existing civilian nuclear technology increases, so does the risk of its diversion and weaponization; and the adoption of new technologies such as spending fuel recycling and fast (breeder) reactors to provide new potential sources of proliferation.

Most of the countries around the world, which are either pursuing nuclear power or currently using it, have signed the NPT and have agreed to comply with rules ensuring that they will not use nuclear technologies toward making weapons. In legal framework there are some critics about the NPT which have basic deficiencies, such as it does not delineate the limits on permissible “peaceful” technology, with respect to fuels that are immediately usable to make nuclear explosives; it sharply restricts IAEA inspections; the treaty’s universality is undermined by India, Israel, North Korea, and Pakistan, which stand as examples of what a state can accomplish outside its strictures and norms.²⁰⁵

Our view has some different ideas. We must remember that the NPT’s legal regime came into force in 1970 and remains the sole internationally accepted medium for reaching diplomatic consensus on nuclear disarmament. It is in essence a ‘bargain’ between States ‘recognized’ as possessing nuclear weapons and those with no such weapons, and is based on three ‘Pillars’ summarized as nuclear non-proliferation; nuclear disarmament; and the right to generate electricity from nuclear reactors for peaceful use. The recognized nuclear weapons states (NWS) are China, France, Russia, UK and US, which are also the sole and veto-carrying permanent members – the P5– of the UN Security Council (UNSC). All are intent on retaining their UNSC status. At least four more states also possess nuclear weapons –India, Israel, North Korea and Pakistan, and there are well-publicized concerns about Iran. India and Pakistan have not signed the NPT: Israel has, but refuses to admit officially that it possesses nuclear weapons. North Korea ratified the NPT but withdrew in 2002. Some

²⁰⁴ Any civilian use of nuclear energy falls within this basic framework established by the NPT, with its recognition in Article IV of an inalienable right of states to pursue peaceful uses of nuclear energy, including development of the full nuclear fuel cycle, as limited by non-nuclear weapon states’ necessary compliance with Articles I, II and III of the treaty, which impose obligations aimed at preventing the proliferation of nuclear weapons. Article III of the NPT requires non-nuclear weapon states to conclude a separate bilateral treaty with the International Atomic Energy Agency (IAEA), under which all fissile materials and all civilian nuclear facilities within the territory of the state will be placed under safeguards administered by the IAEA, to confirm that no fissile material is diverted from peaceful uses to military uses. Article III also provides an international legal mandate for states to individually maintain national export control systems, designed to prevent the spread of materials and technologies that could be used in a military nuclear program, to states and non-state actors of concern. Many national export control systems are coordinated and harmonized through the Nuclear Suppliers Group, a nonbinding multilateral arrangement among supplier states.

²⁰⁵ Victor Gilinsky and Henry Sokolski: “Serious Rules for Nuclear Power Without Proliferation”, *The Nonproliferation Review*, Volume 21, Issue 1, January 2014, pp. 77-98.

non-nuclear weapons states (NNWS) have treaties of ‘protection’ with a NWS, being under a ‘nuclear umbrella’. Non-proliferation has several aspects: stopping the manufacture of new weapons but keeping all or some of the old ones; reducing the current arsenal of weapons, deployed, non-deployed or both; the participation of some or all NWS; and partial or complete disarmament.²⁰⁶

Middle Eastern countries (Iran, the United Arab Emirates, Saudi Arabia, Kuwait, Egypt, and Turkey) are implementing nuclear power programs. According to a new IEA study, the projected cost of generating electricity from nuclear fission has the lowest leveled cost of electricity at discounts rates of 5–10 percent in Europe, OECD-Asia, and North America. Why then were only two large-scale reactors being built in Europe and only two reactors in the final planning stage in the US even prior to the Fukushima disaster in Japan? Mobilizing the typical US\$5 billion capital cost for a large-scale nuclear reactor is an investment that private utilities in liberalized power markets are reluctant to take on.²⁰⁷

European Union

For historical and other reasons, nuclear energy and nuclear safety are regulated somewhat differently from other sectors under EU law. The Treaty establishing the European Atomic Energy Community (the ‘Euratom Treaty’) was adopted in 1957.²⁰⁸ In 2004, the EU Council started a wide-ranging consultation process on the use by member states of existing international instruments on nuclear safety and management of radioactive waste and spent fuel. This eventually led to the establishment of the High Level Group on Nuclear Safety and Waste Management – the European Nuclear Safety Regulators Group (ENSREG). The ENSREG is an independent expert body composed of heads and senior staff members of national nuclear safety or regulatory authorities from all member states as well as a senior

²⁰⁶ None of these options mandate a ban on NW possession, although Article VI of the NPT requires all the NWS to disarm ‘in good faith’. Finer points revolve around ‘maintenance’, ‘upgrading’, ‘modernization’ and ‘renewal’. Arguably, maintenance may be needed to avoid unintentional detonations of weapons with worn-out control and firing mechanisms. New weapon development is partly constrained by the Comprehensive Test Ban Treaty (CTBT) of 1996, which bans full testing but allows ‘sub-critical’ tests. Although ratified by the UK and Russia, the CTBT has not been ratified by eight ‘Annex II’ nations, one of which is the US. Consequently, the CTBT is not yet in force. The US requires conditions to be met before ratification, including the need for careful stewardship of stockpiled weapons. Although technically in force, the NPT is far from achieving consensus, and many NNWS are concerned about a lack of progress. The policy of the P5 is to work ‘step-by-step’. See, Frank Boulton: “Dangers Associated with Civil Nuclear Power Programmes: Weaponization and Nuclear Waste”, *Medicine, Conflict and Survival*, Volume 31, Issue 2, April 2015, pp. 100-122.

²⁰⁷ Marianne Haug, *ibid.*, pp. 92–116.

²⁰⁸ Treaty establishing the European Atomic Energy Community, <http://eur-lex.europa.eu/en/treaties/dat/12006A/12006A.html>, (Accessed on 30.08.2015).

representative from the Commission. In 2007, ENSREG considered whether there was a need for a legally binding instrument on nuclear safety at the EU level.²⁰⁹

Recent years have seen a renewed interest in nuclear energy among European Union (EU) member states. With 144 nuclear power reactors operating in 15 member states, the EU has the largest number of nuclear power plants (NPPs) in the world. At present, nuclear energy provides one-third of the EU's electricity supply and represents 15 percent of the total energy consumed in the EU. The EU Commission considers nuclear safety crucial to member states' decisions on whether to continue to use nuclear energy, as well as for improving public confidence across the EU in the nuclear sector. To achieve these aims, Euratom Council Directive 2009/71 establishing a community framework for the safety of nuclear installations (the 'Directive') was unanimously adopted by the EU Council on June 25, 2009. Despite these shortcomings, the Directive represents a first step towards the adoption of uniform and more detailed community-wide standards concerning nuclear safety in respect of the design, operational and decommissioning requirements. Unlike the IAEA safety standards, which are non-mandatory recommendations, these community safety standards will be legally binding since they will be adopted pursuant to Articles 30 to 32 of the Euratom Treaty.²¹⁰

Of course, after the Cold War era, another important legal framework has been created by signing and implementation of the International Convention for the Suppression of Acts of Nuclear Terrorism and the Convention on the Physical Protection of Nuclear Material along with its 2005 amendment is important for the success of nuclear

²⁰⁹ It was agreed that the following principles would be used to prepare the analysis:

1. Maintain and seek to continuously improve nuclear safety and its regulation, and add value.
2. Just as every member state has the right to decide to use nuclear power or not, so every member state has the right to impose more stringent nuclear safety requirements than those commonly applied.
3. Allow flexibility and not fundamentally change a member state's national nuclear regulatory approach.
4. Seek to enhance, not reduce, the power, roles, responsibilities or capability of the national nuclear regulatory body.
5. Do not expand the role of the Commission in regulatory decision-making or activities or introduce other bodies.
6. Do not divert resources away from national nuclear regulatory responsibilities or international nuclear safety cooperation.
7. Be compliant with the principles/obligations of the Convention on Nuclear Safety.
8. Any proposals should be non-discriminatory towards those who use or do not use nuclear power.
9. Seek to improve the transparency of nuclear safety and its regulation.
10. Be clear on the roles and responsibilities of any organizations involved.

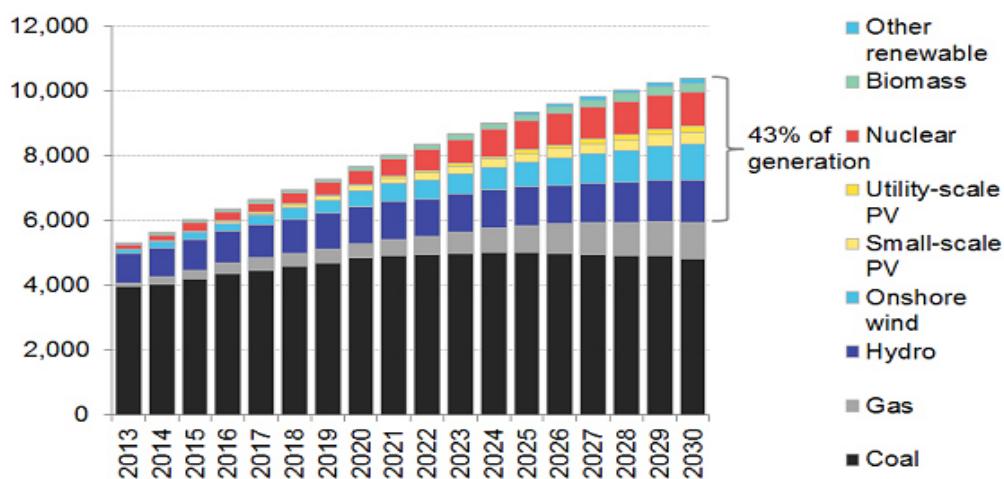
Based on the analysis, in November 2008, the Commission tabled a revised directive on nuclear safety. Subsequent revision of the proposal paved the way for the adoption of the Directive on 25 June 2009.

²¹⁰ Ana Stanič, "EU Law on Nuclear Safety", *Journal of Energy & Natural Resources Law*, 2010, Volume 28, Issue 1, February 2010, pp. 145-158.

security. The regime is meant to universalize or, at least for the time being, promote the wider acceptance of the Code of Conduct on the Safety and Security of Radioactive Sources. Countries have been supporting it and IAEA is well informed of their support.

Turkey and Nuclear Energy Policy Initiatives

In order to ensure its sustainable economic growth, Turkey is planning to benefit from the nuclear power. By this way, it is targeted to decrease the dependence on Tehran and Moscow gas for electricity.²¹¹ Ministry of Energy and Natural Resources of Turkey envisages that the electricity production will be possibly 499 TWh in a high scenario of 8% growth, or 406 TWh with a low one with 6.1% growth. There exist plans for having 30 GWe of coal-fired capacity by 2023, along with 4.8 GWe of nuclear capacity, if everything is planned within its direction. On the other hand, much of Turkey's coal resources do represent as lignite with calorific value –less than 12.5 MJ/kg– and a substantial amount (Afsin Elbistan) at less than 5 MJ/kg (one-quarter of typical steam coal). The Energy and Natural Resources of Turkey has put forward a National Renewable Energy Action Plan. In that plan, share of the renewables in the energy mix by 2023 is expected to be 30%, including 61 GWe to allow safe energy supply and lessen carbon emissions which also comes into meaning that 34 GWe of hydropower, 20 GWe of wind, 5 GWe of solar, 1 GWe of geothermal and 1 GWe of biomass capacity. European Bank for Reconstruction and Development will contribute to the realization of this plan.



Source: http://www.businessspectator.com.au/sites/default/files/11_256.png

Recent developments show that Russia has taken a leading role in offering to finance and build 4800 MWe of nuclear capacity.²¹² Request has been completed for

²¹¹ "Nuclear Power in Turkey - Updated August 2015", <http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/Turkey/>, (Accessed on 30.08.2015).

²¹² Republic of Turkey Ministry of Energy and Natural Resources Nuclear Energy Project Implementation Department, "Turkish Nuclear Power Programme", <http://www.nuclearpowerplantssummit.com/files/Turkish-Nuclear-Power-Programme.pdf>, (Accessed on 30.08.2015).

construction and operating licenses for the first plant, at Akkuyu, and construction works were expected to start in 2015. A Franco-Japanese consortium is going to construct the second nuclear plant, at Sinop. China does represent in agreement to construct the third plant, with US-derived technology. A small uranium mining project is prearranged.



Source: http://www.bgnnews.com/turkey-gives-green-light-to-russian-nuclear-power-plant-project_1916_720_400.jpg

Conclusion

We discussed recent developments in energy security and its future developments above. Nuclear power has a potentially significant role to play in powering the global economy in the coming decades. Considering new nuclear reactor projects and general impulse in the world countries, growing trend in global energy demand over the coming decades and the continued focus on low-emission power solutions, the prospects for an expansion in civilian nuclear power are increasingly realistic. In general, nuclear energy will ignite a renaissance period in the energy sector, offer environmental safety advantages by decreasing the amount of CO₂ and greenhouse effect compared to hydrocarbon fuels, and also will contribute to sustainability and security in energy supplies by ensuring energy diversity. As a result, when we look at the current nuclear energy use and policies of industrial states, we can say that developing countries may use nuclear energy in comply with the legal and international institutional norms, without aiming to produce nuclear weapons in the future. Thus, if we consider possible developments in the medium and long term scenarios from a global energy perspective, nuclear energy sector would consequently play a key role in sustainable energy systems.

- International community needs greater integration of safety and security measures is often straight forward technically.

- Nuclear energy safety and security will be realized with more than some states' monopoly, a multilateral cooperation and partnership structures can handle such a sophisticated task.
- For more powerful nuclear security in the IAEA, as an important part of UN it needs reforms that funding more comprehensive, also it should be more vertical and horizontal representative framework.
- The most reasonable solution was combining multilateralism efforts with the IAEA, which shall results reasonable confidence, more than national self-interests and suspicious tendencies.

REFERENCES

ANDERSON, R., "Nuclear Power: Energy for the Future or Relic of the Past?", BBC, 27 February 2015, <http://www.bbc.com/news/business-30919045>, (Accessed on 30.08.2015).

BOULANIN, V., "International and Legal Frameworks Addressing Cyber Attacks against Nuclear Facilities: The State of Play", CN-228 International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, 1-5 June, 2015, Vienna, Austria, IAEA-CN-228/5A1/138, (Accessed on 30.08.2015).

BOULTON, F., "Dangers Associated with Civil Nuclear Power Programmes: Weaponization and Nuclear Waste", *Medicine, Conflict and Survival*, Volume 31, Issue 2, April 2015.

BOURESTON, J. and OGILVIE-WHITE, T., "Expanding the IAEA's Nuclear Security Mandate", *Bulletin of the Atomic Scientists*, Vol. 66, No. 5, September/October 2010.

"Computer Security at Nuclear Facilities", IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual, International Atomic Energy Agency, Vienna, 2011, http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf, (Accessed on 30.08.2015).

"Convention on the Physical Protection of Nuclear Material", U.S. Department of State Bureau of International Security and Nonproliferation, Signed at New York March 3, 1980, Entered into force February 8, 1987,
<http://www.state.gov/t/isn/5079.htm>, (Accessed on 30.08.2015).

Council of Europe, "Convention on Cyber Crime", Budapest, November 2001,
<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>, (Accessed on 30.08.2015).

CRAIG, P. and GODWIN, S., "*Threat Awareness and Sharing: A Model for Shifting Advantage to the Defender*", International Conference on Computer Security in a

Nuclear World: Expert Discussion and Exchange, 1-5 June, 2015, Vienna, Austria, IAEA-CN-228/PS-II/079, (Accessed on 30.08.2015).

CUNNINGHAM, N., "A Look at the Future of Nuclear Power", *Oil Price*, 24 March 2015, <http://oilprice.com/Alternative-Energy/Nuclear-Power/A-Look-At-The-Future-Of-Nuclear-Power.html>, (Accessed on 30.08.2015).

DAVIS, L. W., "Prospects for Nuclear Power", *The Journal of Economic Perspectives*, Vol. 26, No. 1, Winter 2012.

DUFFEY, R. B., "Sustainable Futures Using Nuclear Energy", *Progress in Nuclear Energy*, Vol. 47, No.1, Issue, 4, 2005.

DUYEON K. and JUNGMIN K., "Where Nuclear Safety and Security Meet", *Bulletin of the Atomic Scientists*, Vol. 68, No.1, January/February 2012.

EBINGER, C. and MASSY, K., "Security Implications of the Expansion of nuclear Energy", *South Asian Survey*, Vol. 17, No. 1, March 2010.

"Energy Security", World Nuclear Association, April 2014, <http://www.world-nuclear.org/info/Economic-Aspects/Energy-Security/>, (Accessed on 30.08.2015).

"Energy Security is National Security - Complete Text TOPIC: Oil & Alternative Fuels, February 28, 2006 Energy Security is National Security, Remarks of Senator Barack Obama Governor's Ethanol Coalition Washington", <http://obamaspeeches.com/054-Energy-Security-is-National-Security-Governors-Ethanol-Coalition-Obama-Speech.htm>, (Accessed on 30.08.2015).

FEDCHENKO, V. and ANTHONY, I., "Nuclear Power and the European Energy Security Strategy", *SIPRI*, June 2015, <http://www.sipri.org/media/newsletter/essay/fedchenko-anthony-june-14>, (Accessed on 30.08.2015).

FUHRMANN, M., "Splitting Atoms: Why Do Countries Build Nuclear Power Plants?", *International Interactions: Empirical and Theoretical Research in International Relations*, Vol. 38, No: 1, 2012, https://www.gwu.edu/~igis/assets/docs/Fuhrmann_Paper.pdf, (Accessed on 30.08.2015).

GILINSKY, V. and SOKOLSKI, H., "Serious Rules for Nuclear Power without Proliferation", *The Nonproliferation Review*, Volume 21, Issue 1, January 2014.

HAUG, M., "Clean Energy and International Oil", *Oxford Review of Economic Policy*, Volume 27, Number 1, 2011.

HULTMAN, N. E., "Risk, Benefit, and Choice: Is Nuclear Power the Answer to Future Energy Constraints?" *Environmental Practice*, Volume 10, Issue 2, June 2008.

IAEA Director General Yukiya Amano, "Introductory Statement to Board of Governors", June 08, 2015, Vienna,
<https://www.iaea.org/newscenter/statements/introductory-statement-board-governors-63>, (Accessed on 30.08.2015).

IAEA Safety Standards for protecting people and the environment "Fundamental Safety Principles, Safety Fundamentals No SF-1", http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf, (Accessed on 30.08.2015).

JOHNSON, T., "Nuclear Power Safety Concerns", Council on Foreign Relations, 23 September 2011, <http://www.cfr.org/world/nuclear-power-safety-concerns/p10534>, (Accessed on 29.08.2015).

JOYNER, D. H., "Nuclear Power Plant Financing Post-Fukushima, and International Investment Law", Forthcoming, *Journal of World Energy Law & Business*, Issue 4, 2013.

KOOTEN, C., JOHNSTON, C. and WONG, L., "Wind versus Nuclear Options for Generating Electricity in a Carbon-Constrained World: Strategizing in an Energy-Rich Economy", *American Journal of Agricultural Economics*, Vol. 95, January 2013.

NICOLL, A., "Nuclear Security after Fukushima", Strategic Comments, Vol. 17, No: 6, 2011, <https://www.iiss.org/en/publications/strategic%20comments/sections/2011-a174/nuclear-security-after-fukushima-c823>, (Accessed on 30.08.2015).

"Nuclear Power in the World Today", World Nuclear Association, Updated February 2015, <http://www.world-nuclear.org/info/Current-and-Future-Generation/Nuclear-Power-in-the-World-Today/>, (Accessed on 29.08.2015).

"Nuclear Power in Turkey - Updated August 2015", <http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/Turkey/>, (Accessed on 30.08.2015)

"Nuclear Proliferation: Risk and Responsibility", The Trilateral Commission, 2006, <http://trilateral.org/download/doc/nuclear.pdf>, (Accessed on 29.08.2015).

"Nuclear Security - Measures to Protect Against Nuclear Terrorism Amendment to the Convention on the Physical Protection of Nuclear Material Report by the Director General, Board of Governors General Conference GOV/INF/2005/10-GC(49)/INF/6 Date: 6 September 2005",
<https://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf>, (Accessed on 30.08.2015).

PASQUALETTIA, M. J., SOVACOOL, B. K., "The Importance of Scale to Energy Security", *Journal of Integrative Environmental Sciences*, Vol. 9, No: 3, 2012.

"Plans for New Reactors Worldwide", World Nuclear Association, May 2015, <http://www.world-nuclear.org/info/Current-and-Future-Generation/Plans-For-New-Reactors-Worldwide/>, (Accessed on 30.08.2015).

PEOPLES, C., "New Nuclear, New Security? Framing Security in the Policy Case for New Nuclear Power in the United Kingdom", *Security Dialogue*, Vol. 45, No: 2, 2014.

RAMEY, J. T., "The Promise of Nuclear Energy", *The Annals of the American Academy of Political and Social Science*, Vol. 410, No.1, November 1973.

RASHAD, M. and HAMMAD, F. H., "Nuclear Power and the Environment: Comparative Assessment of Environmental and Health Impacts of Electricity-Generating Systems", *Applied Energy*, Vol. 65, 2000,
<http://www.emp.rpi.edu/hartford/~odells2/EP/Other/references/Nuclear%20power%20and%20the%20environment,%20comparative%20assessment%20of%20environmental%20and%20health%20impacts%20of%20electricity-generating%20systems.pdf>, (Accessed on 30.08.2015).

Republic of Turkey Ministry of Energy and Natural Resources Nuclear Energy Project Implementation Department, "Turkish Nuclear Power Programme",
<http://www.nuclearpowerplantssummit.com/files/Turkish-Nuclear-Power-Programme.pdf>, (Accessed on 30.08.2015).

ROSEN, M. A. and DINCER, I., "Nuclear Energy as a Component of Sustainable Energy Systems", *International Journal of Low Carbon Technologies*, Vol. 2, No: 2, 2007, <http://ijlct.oxfordjournals.org/content/2/2/109.full.pdf+html>, (Accessed on 30.08.2015).

SARKISSIAN, A., BIROL, F., "Can Nuclear Energy Fuel Our Future?", *World Economic Forum Agenda*, 10 November 2014,
<https://agenda.weforum.org/2014/11/can-nuclear-energy-fuel-our-future/>, (Accessed on 29.08.2015).

"Sustainable Energy", Nuclear Energy Association, June 2013, <http://www.world-nuclear.org/info/Energy-and-Environment/Sustainable-Energy/>, (Accessed on 30.08.2015).

STANIČ, A., "EU Law on Nuclear Safety", *Journal of Energy & Natural Resources Law*, 2010, Volume 28, Issue 1, February 2010.

"The Interface Between Safety and Security at Nuclear Power Plants", A Report by the International Nuclear Safety Group, INSAG-24, International Atomic Energy Agency, Vienna, 2010, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1472_web.pdf, (Accessed on 30.08.2015).

Treaty Establishing the European Atomic Energy Community, <http://eur-lex.europa.eu/en/treaties/dat/12006A/12006A.html>, (Accessed on 30.08.2015).

WICKS, M., "Energy Security is not a Luxury but a Necessity in a Dangerous World", *The Telegraph*, 5 April 2010,

<http://www.telegraph.co.uk/finance/comment/7556841/Energy-security-is-not-a-luxury-but-a-necessity-in-a-dangerous-world.html>, (Accessed on 30.08.2015).

WINTER, G., "The Rise and Fall of Nuclear Energy Use in Germany: Processes, Explanations and the Role of Law", *Journal of Environmental Law*, Vol. 25, No: 1, 2013.

CYBER SECURITY OF NUCLEAR POWER PLANTS

Guido GLUSCHKE

ABSTRACT

The threat from cyber attacks is increasingly perceived as a problem of national and international security, as these attacks grow in number and sophistication, and as perpetrators are no longer just private hackers or organized criminals, but also nation states. Likewise, attacks once confined to standard computer systems have now been extended to instrumentation and control (I&C) systems with all the implications and potential consequences of such attacks.

In order to understand the implications and consequences for nuclear power plants (NPPs), cyber security domains are introduced. These domains group the various types of computer systems into functional elements, which can then be better understood in terms of their importance for a NPP. To ensure an up-to-date view on cyber security, considerations on new NPP operation models are also set forth. The new operational models entail new threats to the cyber threat landscape.

Cyber attacks pose a real threat to the energy sector, and a more substantial assessment of relevant cyber security threats is provided through a closer analysis of technology issues, as well as systemic threats and threats stemming from human factors. Furthermore, the widely used threat-assessment model Design Basis Threat (DBT) is discussed in terms of its limits for cyber security. A view on risk management and risk modeling is presented.

Cyber security has become an essential component of the overall security framework of nuclear facilities, and this emerging area is a growing priority for facility operators, national regulators, and international organizations such as the IAEA. This paper is focused on elements and requirements for cyber security in national regulation as well as operational governance for NPPs.

Finally, this study includes concepts for implementing cyber security at nuclear facilities. Beyond the traditional approach to prevention, detection and response, additional aspects are discussed, such as security management, capacity building and nuclear security culture.

Key Words: Cyber Security Domains, NPP Operation Models, Cyber Security Threats, DBT, Regulatory Framework, Security Management, Capacity Building, Nuclear Security Culture

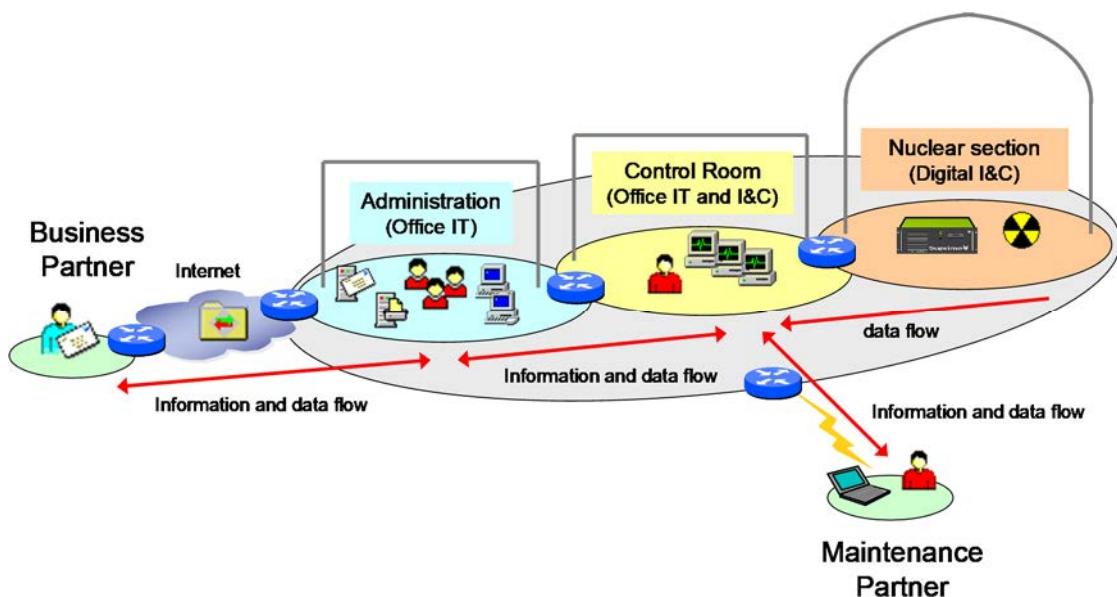
Introduction

Today, all industries are becoming increasingly digitized. The energy and the nuclear sector are no exception. Information and communication technology is a part of most business processes, and influences the nuclear industry in the same way as it does other industries. However, the nuclear sector differs from other industries because it is highly regulated, and thus technical developments cannot be implemented in the same way as in other industries. In light of recent trends, such as cloud services or mobile devices, information technology in general is a big challenge for the nuclear industry. This article deals with cyber security issues at nuclear facilities and focuses in particular on nuclear power plants (NPPs). In the literature, the terms 'cyber security', 'IT security' and 'computer security' describe security of information assets or digital systems.²¹³ In the current paper, the term 'cyber security' will be used as the general term.

Cyber Security Domains in Nuclear Power Plants

In order to provide a better understanding of the information flow in a nuclear power plant, Figure 1 shows the general information and data exchange between different sections of a NPP.

Figure 1. Information flow in a NPP



The administrative domain of a NPP works with standard business information technology (IT) and is comparable to business IT found in other industries. Typically, data from management, human resource, logistics or procurement are processed in this section. There are also systems for office automation, e.g. email, file and print

²¹³ Tim Maurer and Robert Morgus, "Compilation of Existing Cyber Security and Information Security Related Definitions", *New America Foundation Report*, October 2014.

services, engineering and maintenance systems, workflow systems or document management systems. Systems for access and badge management might also be part of the administrative section. These systems are partly used in the second domain, the control room.

Figure 2. Nuclear power plant control room for operators²¹⁴

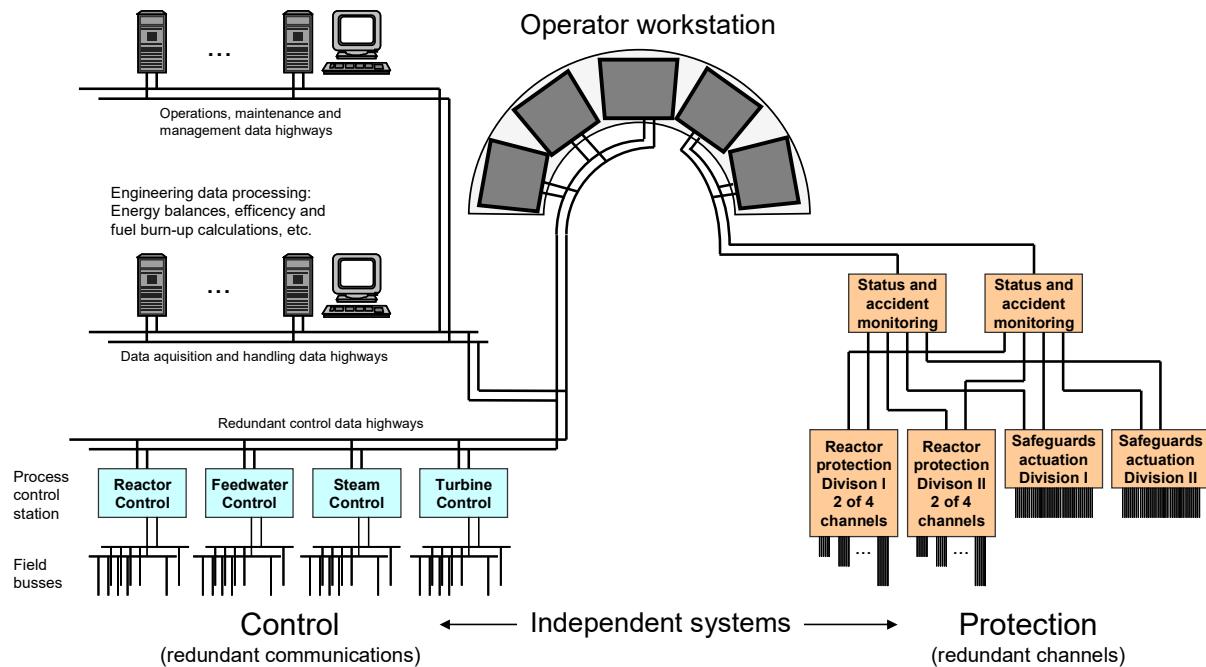


The control room is usually connected both to the administrative systems²¹⁵, including email or document management, and to systems controlling the plant equipment and for protecting the nuclear section as shown in Figure 3.

²¹⁴ International Atomic Energy Agency, “Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants,” *IAEA Nuclear Energy Series*, No. NP-T-3.12, Vienna, 2011.

²¹⁵ International Atomic Energy Agency, *IAEA Nuclear Security Series No. 17 – Computer Security at Nuclear Facilities*”, Vienna 2011.

Figure 3. Example of nuclear power plant control room I&C structure



Systems for the operational control of a NPP are, for example, reactor control systems but also feedwater, steam or turbine control systems. Additional systems are installed to protect the plant against unwanted occurrences. These safety systems, such as reactor limitation or protection systems, are designed, for instance, to ensure a safe shutdown of the reactor in order to prevent a core melt. The aforementioned systems are part of the plant instrumentation and control (I&C).

Furthermore, there are emergency systems to support the operation of the plant in an emergency, such as fire protection systems and voice and data communication infrastructure. All these systems include digital components, which must be considered when developing the cyber security architecture.

Threat and Risk Modelling

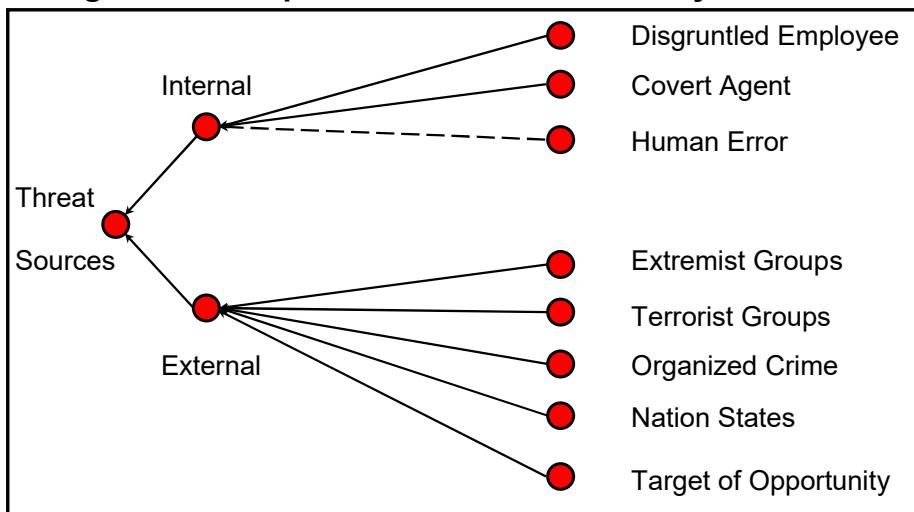
In many countries, nuclear power plants are seen as a part of the critical infrastructure. With that in mind, they could be a target for professional adversaries. As a consequence, nuclear facilities have to deal with many risks regarding IT and I&C.²¹⁶ To understand the sources of risks in terms of nuclear security, it is essential to discuss the various threats and impacts that come into play when operating IT/I&C in a nuclear facility. From the perspective of the state and the operator, the most important source for IT-based threats is the Design Basis Threats (DBT) assessment, which is

²¹⁶ Caroline Baylon, “Cyber Security at Civil Nuclear Facilities – Understanding the Risks”, *Chatham House Report*, London, September, 2015.

conducted at the state level. “A DBT is the State’s description of a representative set of attributes and characteristics of adversaries, based upon (but not necessarily limited to) a threat assessment, which the State has decided to use as a basis for the design and evaluation of a physical protection system. A DBT is a comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated.”²¹⁷

A threat is the combination of capability, intent and opportunity. A threat assessment requires threat sources are that combine capabilities and motivation. Examples of threat sources are shown in Figure 4. Then, the capability of a particular threat source can be evaluated. Obviously, one important aspect for evaluating threat capability is knowledge about attack vectors or about groups who develop and deliver malicious code for attacks. Another aspect could be the financial resources necessary to buy malicious code, which can easily cost up to \$50,000. The “Target of Opportunity” is unique to cyber threats. This means that a nuclear installation is accidentally, rather than deliberately, hit by a cyber attack. But even this scenario must be considered seriously.

Figure 4. Examples of threat sources for cyber threats



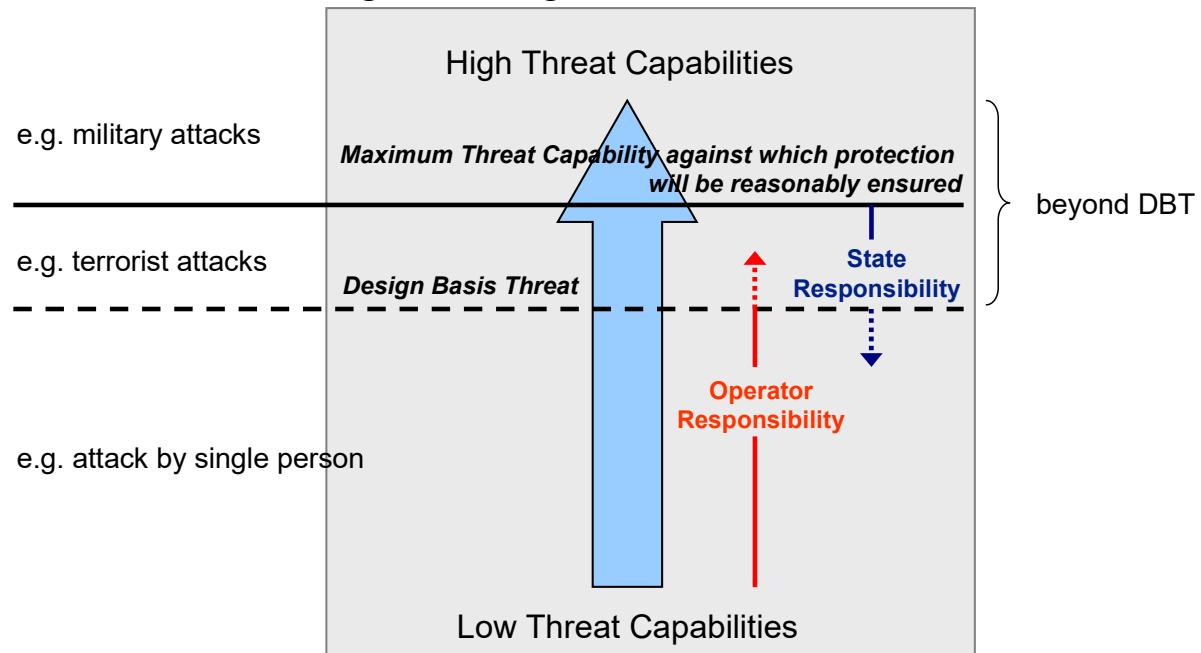
Part of the DBT methodology is the process of determining which threats are the responsibility of the operator, and which must be addressed by the nation state. It is obvious that not all threats can be borne by the operator. In nation states, the fight against terrorism is typically the responsibility of the state.

In the physical world for which the DBT methodology was designed, the “Maximum Threat Capability” can be clearly defined. Assumptions about the capability of a physical attacker with his weapons or explosives can be made, and these may exceed the defense capacity of the operator. Such threats are deemed “beyond DBT”.

²¹⁷ International Atomic Energy Agency, “IAEA Nuclear Security Series No. 10 – Development, Use and Maintenance of the Design Basis Threat”, Vienna, 2009.

Considering DBT, there are three essential questions in regard to cyber security: (i) What is the maximum threat capability of a cyber threat agent? (ii) How can we determine whether a cyber attack is a terrorist act? (iii) How can we define and describe the level of cyber threat for which the state must bear responsibility? These and other questions are intensively discussed at the IAEA, but they are not answered finally by now. The DBT model is shown below:²¹⁸

Figure 5. Design Basis Threat Model



Beside specific threats evaluated by the nation state and its security agencies, the question remains whether cyber is a new threat actor or whether cyber is only a tool which is used by existing threat actors. A structured DBT could cover attack groups, such as

- Terrorism;
- Insider;
- Organized Crime;
- Environmental Activists, or
- Other.

Cyber issues can apply to all attack groups mentioned above. But one group is not mentioned in the DBT for physical security: the military attack group. The reason why

²¹⁸ Guido Gluschke and Andrea Cavina, "Translating the DBT: A Comparative Analysis", *International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange*, Vienna, 1-5 June, 2015.

military weapons are not covered by the DBT, or being more precise, are not assigned to the licensee's responsibility is because

- (a) in general, military weapons are controlled by nation states;
- (b) nation state's intelligence service is responsible for tracking such a threat if it becomes real;
- (c) nation state's armed forces should be able to fend off such kind of threat.

In the western hemisphere military attacks can be categorized as 'beyond state' for attacks using kinetic military weapons. But is this true for cyber? A cyber weapon can be launched by everybody with the right skills. So, we have to take into account that there are military-grade cyber weapons available in the hands of adversaries. That is the reason why military should become a new DBT threat group in terms of cyber.

The three aspects regarding physical military attacks mentioned above cannot be seen as effectively controlled in cyber, because:

- (a) Cyber weapons cannot be controlled by nation states. In general, everybody who has sufficient capability and knowledge can produce a sophisticated and effective cyber weapon. Technically, it is only necessary to have a PC, an internet connection and software development kits for the target systems which should be attacked and which can be usually downloaded from the internet;
- (b) Once somebody has such a cyber weapon he becomes a real threat but most national intelligence services have not the capabilities and opportunities for tracking such kind of cyber threats or threat actors. Old school methods of investigation or surveillance are not working any longer;
- (c) In case of a physical military weapon not detected by intelligence services and moved near to a nuclear facility in order to attack it the assumption exists that such a single attack can be warded off by armed forces while a sophisticated cyber attack would most likely not be fended off by a nation state. In addition, attribution of a professional cyber attack is hardly possible. In consequence, neither effective detection nor adequate response is given. Looking to Stuxnet, in a three months period after its appearance in June 2010 nobody had a clear understanding whether this cyber weapon was used against him.

The main characteristic of a cyber weapon is its effectiveness. Military-grade cyber weapons are highly targeted and highly effective like bunker buster bombs in the physical world. Highly effective means that the cyber weapon leads to a successful

attack with a high probability. Looking at a comment on Stuxnet published in the NYT²¹⁹: "To check out the worm, you have to know the machines," said an American expert on nuclear intelligence. "The reason the worm has been effective is that the Israelis tried it out."

The manufacturing of military-grade cyber weapons is very expensive. This depends not only on the zero-day-exploits which are part of it but also on the fact that this kind of cyber weapon has a limited lifetime. Once used, a single cyber weapon is no longer a threat for the targeted facility because after a phase of forensics the targeted facility knows how to respond to this attack vector. It is a weapon with a one-off effect when there is a response team with adequate knowledge. Right now, the sources of such threats can be assumed to be nation states because a huge amount of resources and a multi-year military-like planning is necessary to build a cyber weapon such as Stuxnet. At the moment a handful countries are suspected to have military-grade cyber weapons for offensive use. At least the same amount of countries has the capability to do so, but the number will be rising soon²²⁰.

If an attack fails in the physical world the attacker can use more powerful weapons and try it again. If he has more powerful weapons then there will be a point in time when he is successful. In the digital world an approach which is based on physical power only works in very rare cases, e.g. in case of brute force attacks in order to break crypto keys. The success of cyber attacks is not depending on the question of how powerful a weapon is but of how sophisticated it is. That means the game will be won by the most creative and effective attacker or defender. And it will be won by the party who has an entire attack or risk view, sufficient experience and situational awareness as well as suitable methods for attacking or mitigating. Methodologies known from the physical area regarding robustness of protection measures are not applicable any more. Defining a threshold value for the number of attackers, amount or type of weapons is not sufficient for cyber. A new way to define a level of cyber threat, or cyber power, must be found.

The question remains what a "Maximum Threat Capability" is in terms of cyber and how to describe the parameters which make a nation state to a powerful nation state in the age of cyber. Everybody would say: "We are as secure as possible from our perspective, considering our means and our knowledge". This includes a couple of limits, such as:

²¹⁹

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&pagewanted=all

²²⁰ Scott Borg, Director and Chief Economist of the U.S. Cyber Consequences Unit (US-CCU), Talk at DGAP, Berlin, January 2012.

- Limits of informatics, mathematics, physics;
- Limits of methodology, human imagination and knowledge during the design process, e.g. single point of failure, common cause failures, insufficient methods;
- Limits of vendors and supply chain, e.g. quality limitation in implementation of hardware and software, trusted supply chain;
- Limits of verification and testing, e.g. no error free software;
- Limits of detection and response, e.g. limited technics for detection, limited capabilities, knowledge and experience, missing situational awareness.

These limits can be seen as restrictions in order to defend against cyber threats successfully. In consequence, the "Maximum Threat Capability" in terms of cyber could be considered as "Cyber-related threats, a nation state is unable to defeat", such as:

- Denial of Service (DoS): When a nation state is not capable to handle massive DoS attacks;
- Encryption: When a nation state is not capable to evaluate if an encryption is strong enough for its intended purpose;
- Advanced Persistent Threat (ATP): When a nation state has no detection or protection mechanisms regarding zero day exploits;
- Malware: When a nation state has no antivirus industry which detects in higher quality than the commercial AV scanners;
- Supply Chain: When a nation state is not able to check if IT/OT systems or software for critical sectors are free of backdoors or hidden functions when bought from sources in other countries.

This list shows some limits vital for a nation state to control the threats stemming from the ongoing digitalization of critical infrastructure sectors, such as energy and nuclear.

Cyber Security Threats

The following threats are to be considered as general sources of risks, including internal and/or external attackers – but it is crucial not to reduce the threats and threat actors to external attacks Internal attacks have to be considered, too.

- Theft:
 - Espionage through unauthorized access to information
 - Theft of IT/I&C equipment, mobile devices or mobile storage (e.g. USB-sticks, CDs)

- Misuse:
 - Misuse/abuse of IT or I&C equipment (e.g. unauthorized granting of access rights)
- Manipulation:
 - Manipulation of data, communication equipment, IT systems, I&C components through malware (e.g. virus, worm or Trojan horse)
 - Manipulation of data, communication equipment, IT systems, I&C components through human actions (e.g. change configuration, lock down a system, open a firewall port)
- Destruction:
 - External attack against IT/I&C through hackers (e.g. sending “logical bombs” or conducting a denial-of-service attack)
 - Physical violence against IT/I&C through human actions (e.g. destroying computers or cables)

As a first step, it is essential to find out which vulnerabilities are relevant for making a particular threat “successful”, and which IT/I&C flaws are exposed through a single vulnerability combined with a single threat. These vulnerability-threat-combinations are the foundation for evaluating risks.

The next step is to identify which vulnerability-threat-combinations can impact the nuclear plant. An impact analysis should be performed to find out whether a threat could influence the safety, security or operation of a nuclear facility. Therefore, it is essential to fully understand all IT and I&C functions at the plant. In addition to single vulnerability-threat-combinations, it is also important to analyze the dependencies of the IT/I&C components, and to identify which common cause failures they could cause.

Threat and Risk Mitigation

The protection of nuclear facilities is the responsibility of nation states. Most countries follow the IAEA recommendations on physical protection, NSS13.²²¹ From the nuclear security perspective, nuclear computer security goals can be derived from the NSS13. Computer security is focused on preventing computer actions that could directly or indirectly lead to

- unauthorized removal of nuclear or other radioactive material;
- sabotage against nuclear material or nuclear facilities;
- theft of nuclear sensitive information.

²²¹ International Atomic Energy Agency, “IAEA Nuclear Security Series No. 13 – Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)”, Vienna 2011.

These nuclear computer security goals describe possible scenarios that must be avoided. Thus, the goals have to be met by the regulator as well as the operator. There may be a cyber regulation that sets forth the necessary steps for achieving the safe and secure operation of a nuclear facility. This is not always the case, though. The level and scope of cyber regulation differs from country to country.²²²

An essential step towards increasing security is to identify and understand digital systems that are vital for the operation of the plant and for handling emergency situations. Essential digital systems comprise not only safety systems, safety-relevant systems, and emergency systems, but also, potentially, particular operational systems. These systems have to be identified and classified in regard to their contribution to protection against potential threats.

Vulnerability assessments must be conducted to evaluate the ways in which nuclear computer security goals can be violated in a particular nuclear installation. These vulnerability assessments have to take into account that a computer system can be a source of a cyber threat, a target of a cyber threat, or the means by which a cyber threat is launched. In addition to technical components and computer systems, information should also be considered as a vital asset. Manipulated information, paper or digital, can seriously impact systems, processes, and workflows. Security assessments should consider how information leads to decision-making, in addition to the impact on the nuclear security goals, as well as the nuclear computer security goals.

An information or computer risk assessment will evaluate all the relevant scenarios for the nuclear facility. These will include all the scenarios that could impact nuclear computer security aims, but can also be extended to additional operator-specific risks, such as breaches of information about customers or suppliers.

National Legislative and Regulatory Framework

The IAEA's nuclear security framework sets forth 12 essential elements of a Nuclear Security Regime.²²³ One of these elements is the "Legislative and Regulatory Framework", which has to be established by the nation state. Regulatory functions could comprise:

- Establishment of national safety and security requirements and regulations
- Licensing system with regard to nuclear installations

²²² Guido Gluschke and Andrea Cavina, "Cyber Security at Nuclear Facilities: National Approaches, Study of the Institute for Security and Safety at the Brandenburg University of Applied Sciences", Potsdam, July 2015.

²²³ International Atomic Energy Agency, "IAEA Nuclear Security Series No. 20 – Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime", Vienna 2013.

- System of regulatory inspection and assessment of nuclear installations
- Enforcement of applicable regulations and of the terms of licenses
- Regulatory safety and security research
- Monitoring of safety events, operating experience and implementation
- Monitoring of security events (incidents) and threat level
- Radiation protection, environmental monitoring
- Emergency preparedness
- International co-operation

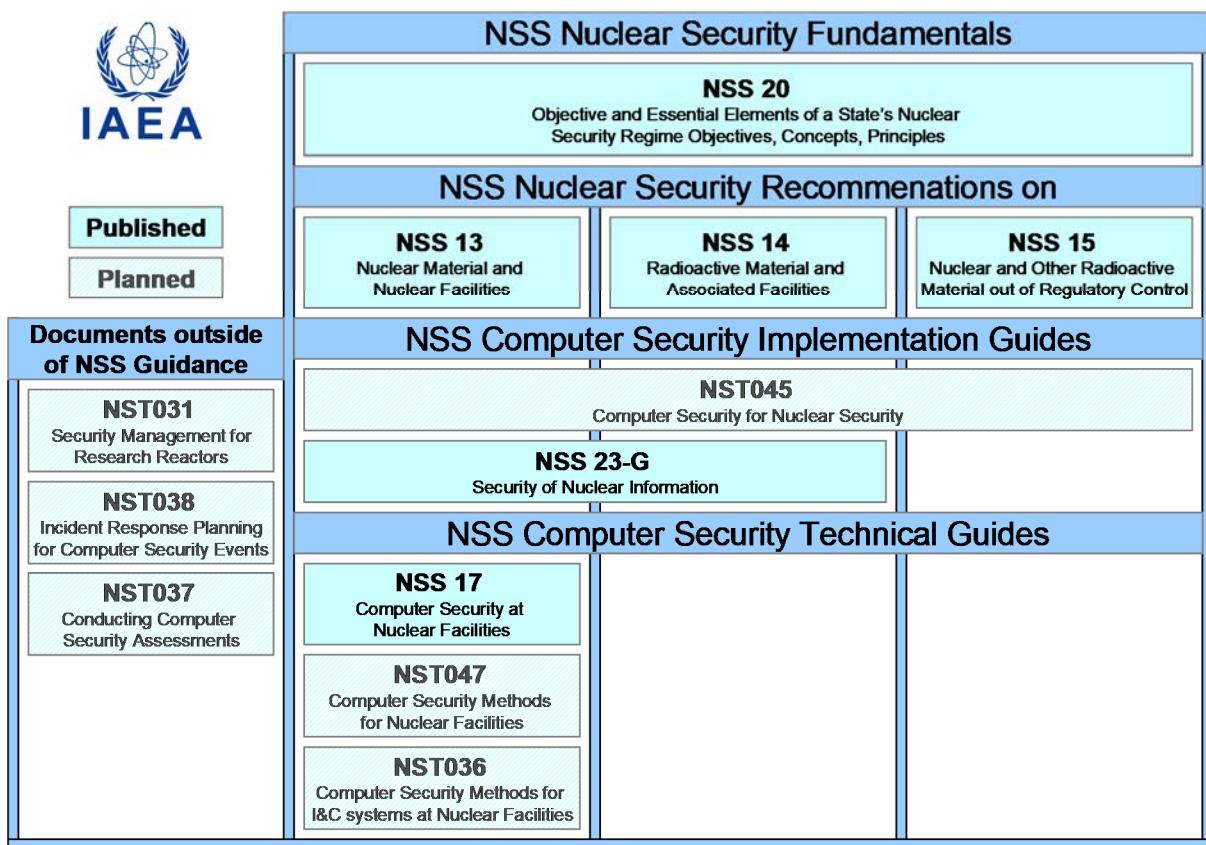
Cyber security should be considered a part of all of these functions. To support states in these efforts, the IAEA is working on cyber security guidance documents.²²⁴ These documents are based on the three pillars defined within the IAEA recommendation documents:

- Nuclear Security Recommendations on Nuclear Material and Nuclear Facilities (NSS13)
- Nuclear Security Recommendations on Radioactive Material and Associated Facilities (NSS14)
- Nuclear Security Recommendations on Nuclear and other Radioactive Material out of Regulatory Control (NSS15)

NSS13 and NSS14 address nuclear and radioactive material within regulatory control. An overview of these documents can be found below:

²²⁴ Donald D. Dudenhoeffer, Khammar Mrabit, John Hilliard, and Michael T. Rowland, "Gates, Guards, Guns And Geeks: The Changing Face Of Nuclear Security And The IAEA's Leading Role In Promoting Computer Security For Nuclear Facilities", *9th International Topical Meeting on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC & HMIT 2015)*, Charlotte, February 23-26, 2015.

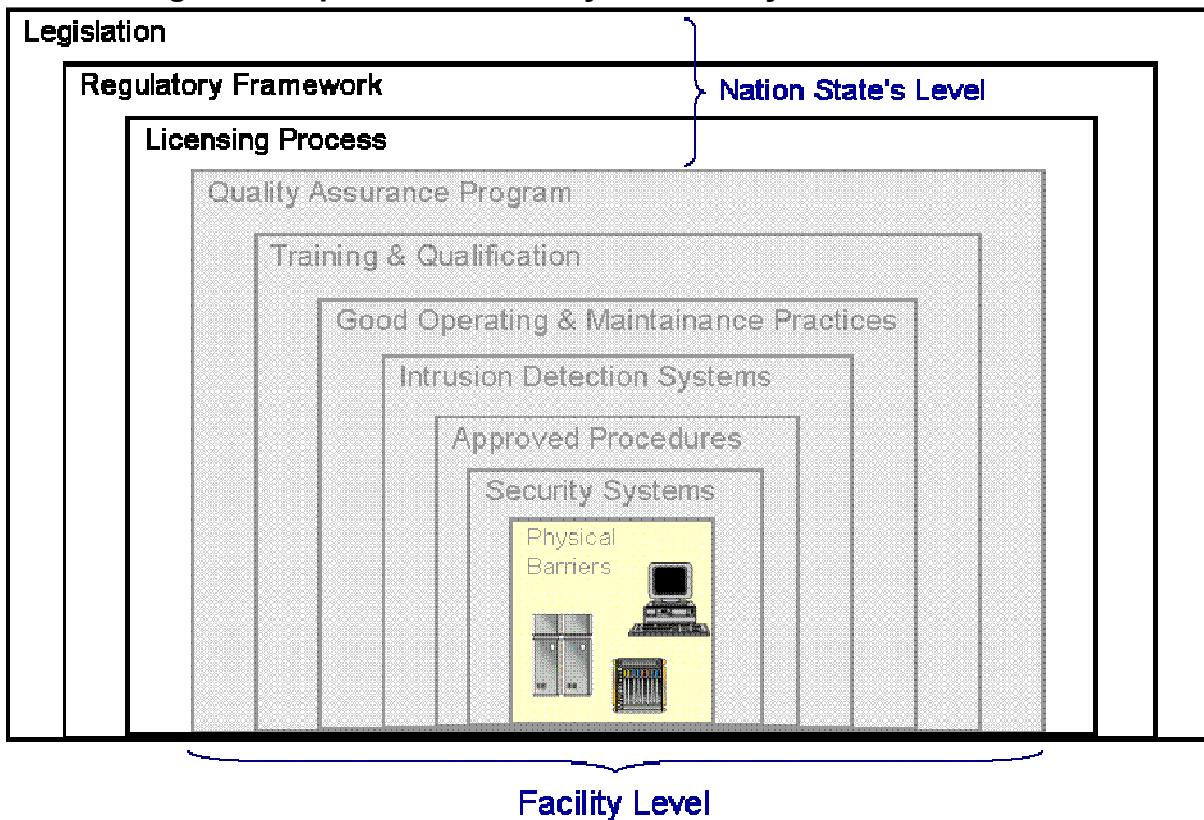
Figure 6. IAEA Computer Security Guidance Overview



To ensure cyber security at nuclear facilities, national legislation must be in place. Cyber security legislation could fall under within the legislation for the nuclear sector, though it is often provided as independent legislation.²²⁵ A national regulatory framework should include cyber security requirements. Furthermore, cyber security should be part of the licensing process for a nuclear facility.

²²⁵ Guido Gluschke and Andrea Cavina, "Cyber Security at Nuclear Facilities: National Approaches", *Study of the Institute for Security and Safety at the Brandenburg University of Applied Sciences*, Potsdam, July 2015.

Figure 7. Implementation of cyber security in nuclear facilities



The operator must implement the requirements imposed by the regulatory framework in conjunction with the DBT. The essential elements for a nuclear security regulation in the nuclear sector may be a cyber security concept or a computer security plan.²²⁶ The essential elements include:

- Define organizational framework for computer security
- Determine resources, roles and responsibilities
- Identification of all computer systems and related processes in a facility that can contribute to a malicious act
- Assigning computer security levels to computer systems
- Determination of computer security zones
- Determination of necessary computer security measures
- Plan for realization of computer security measures

The computer security concept needs to be tailored to the current situation at the facility, must be evaluated regularly, and should cover the whole life cycle of computer systems. Additionally, human resource development and capacity building in cyber security is crucial in order to establish a robust cyber security approach at a nuclear

²²⁶ International Atomic Energy Agency, "IAEA Nuclear Security Series No. 17 – Computer Security at Nuclear Facilities", Vienna 2011.

facility.²²⁷ Moreover, information security management and a security culture contribute significantly to nuclear cyber security.

Future Perspectives

In the past, nuclear power plants were run by state organizations or the companies that own the plants. For the most part, these organizations oversee the development of their plants and are very familiar with all details of the plant, its operation, and maintenance. In light of the latest developments on the market for nuclear power plants, a new operational model has become more and more popular: the “turnkey” solution. Under this model, the vendor of the nuclear power plant remains the owner of a particular part of the facility, mostly by holding the majority of shares. In this case, the NPP is run by the vendor. These issues are the subject of negotiation between the vendor and its customer. Simply put, the organization that buys the NPP from this vendor becomes the owner of the remaining shares, and additionally gains access to the energy that is produced by the NPP in its country.

Now, with this new mode of operation, a limited know-how transfer takes place between the vendor and the organization responsible for the NPP in its country, i.e. the national operator. Moreover, not only does the operator have limited information about the NPP, the regulator has also limited access to knowledge about this plant.

This situation makes it difficult to develop adequate regulations for the nuclear power plant, in particular for the cyber sections of a modern plant. As mentioned above, digital components are increasingly common, even if they are not visible. However, robust regulation in terms of safeguarding, safety and security is key to the secure and safe operation of a nuclear power plant. The IAEA provides guidance on computer security issues and involves nation states in active discussions to improve international awareness, understanding, training and education in terms of cyber security.

Another aspect of this development is dependency on communication, and in particular the need for communication between the NPP and the vendor, which is typically located in another country. The vendor wants performance or maintenance data for the plant and may adjust equipment settings in order to improve performance or correct errors. These exchanges of data require connectivity and will be mostly conducted online. Thus, in peacetime, the question can be reduced to the reliability of internet connections. In wartime, the availability of internet connections in general may be an issue. From the international perspective, the question arises whether the internet constitutes part of a nation state’s critical infrastructure. This leads to considerations of dependencies and derived critical scenarios.

²²⁷ Guido Gluschke and Andrea Cavina, “Educational Instruments for Nuclear IT/Cyber Security and Information Security Capacity Building”, *International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange*, Vienna, 1-5 June, 2015.

REFERENCES

BAYLON, C., "Cyber Security at Civil Nuclear Facilities – Understanding the Risks", Chatham House Report, London, September 2015.

DUDENHOEFFER, D. D., MRABIT, K., HILLIARD, J. and ROWLAND, M. T., "Gates, Guards, Guns And Geeks: The Changing Face Of Nuclear Security and the IAEA's Leading Role in Promoting Computer Security for Nuclear Facilities, 9th International Topical Meeting on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC & HMIT 2015)", Charlotte, February 23-26, 2015.

GLUSCHKE, G. and CAVINA, A., "Educational Instruments for Nuclear IT/Cyber Security and Information Security Capacity Building", International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, Vienna, June 1-5, 2015.

GLUSCHKE, G. and CAVINA, A., "Translating the DBT: A Comparative Analysis", International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange, Vienna, June 1-5, 2015.

GLUSCHKE, G. and CAVINA, A., "Cyber Security at Nuclear Facilities: National Approaches", Study of the Institute for Security and Safety at the Brandenburg University of Applied Sciences, Potsdam, July 2015.

IAEA, "Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants", IAEA Nuclear Energy Series NP-T-3.12, Vienna, 2011.

IAEA, "IAEA Nuclear Security Series No. 10 – Development, Use and Maintenance of the Design Basis Threat", Vienna, 2009.

IAEA, "IAEA Nuclear Security Series No. 13 – Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities" (INFCIRC/225/Revision 5), Vienna, 2011.

IAEA, "IAEA Nuclear Security Series No. 17 – Computer Security at Nuclear Facilities", Vienna, 2011.

IAEA, "IAEA Nuclear Security Series No. 20 – Nuclear Security Fundamentals: Objective and Essential Elements of a State's Nuclear Security Regime", Vienna, 2013.

MAURER, T. and MORGUS, R., "Compilation of Existing Cyber Security and Information Security Related Definitions, New America Foundation Report", October 2014.

CYBER SECURITY FOR NUCLEAR INSTALLATIONS

A. Beril TUGRUL

ABSTRACT

Nuclear security is fundamental concept in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported. It involves preventing, detecting, and responding to criminal or intentional unauthorized activities. Additionally, nuclear security deals with actions involving or directed at nuclear material, other radioactive material, associated facilities, or other activities that could directly or indirectly produce harmful consequences to persons, property, society or the environment. The nature and range of threats to security have become extremely complex and unpredictable, and remain of vital importance for the nuclear sectors. In this study, the complexity, components, and importance of the cyber security for nuclear facilities are analyzed. The paper argues that some essential cyber security processes should be handled both technically and administratively.

Key Words: Computer Security, Cyber Security, Nuclear Installation, Security

Introduction

Energy supply security is vital for all states due to the potential impact on economic, geopolitical and political dimensions. Therefore, energy policies adopted as state policies are emphasized.²²⁸ In terms of energy policies, fossil fuel or nuclear power plants have primary importance in energy supplies for states.

Nuclear facilities must meet certain conditions to comply with industry and energy policy. In order to construct and operate a nuclear installation, it is compulsory to obtain a license from the Authority. Here, the term "Nuclear Installation" refers to nuclear reactors and nuclear fuel cycle facilities. "Nuclear Reactor facilities" consist of: all type reactors (e.g. training reactors, research reactors, material testing reactors, test reactors, prototype reactors, reactors for heat production and reactors for electrical power production. Nuclear power plants are also very important for energy security,

²²⁸ Beril Tugrul, "Decision Making Process in Energy Policies", Yıldız Technical University-YTU, Political Science and International Relations-PSIR Bulletin, No: 11, Summer, 2015, pp. 10-13.

and it is expected that their number will increase in the future due to sustainable development via a society that has no effect on climate change.²²⁹ As a consequence, the number of other nuclear facilities (e.g. supplying fuels and other activities) will also increase.

“Nuclear Fuel Cycle Facilities” comprise mining, milling and refining facilities, conversion facilities, enrichment facilities, nuclear fuel element fabrication facilities, reprocessing facilities for used fuel elements and radioactive waste management facilities for processing radioactive waste (including ultimate storage).²³⁰ Therefore, the term nuclear installation includes all types of facilities for nuclear technology, and all of them have strategic priority for the nuclear industry.

In order to construct and operate a nuclear installation, a license must be obtained from the National Authority. Therefore, the applicant has to submit an application to the National Authority describing the nature of the installation to be constructed and the implementer’s technical and financial capacity.²³¹ International inspection is also compulsory for many countries.

For nuclear installations, nuclear security is a fundamental concept in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported. It involves preventing, detecting, and responding to criminal or intentional, unauthorized activities. Additionally, nuclear security deals with actions involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities that could directly or indirectly produce harmful consequences to persons, property, society, or the environment.

Security Supply for Nuclear Installations

Nuclear installations offer many benefits, ranging from power generation and related activities. Nuclear power generation is of vital importance for states due to the huge energy production capacity of a single plant. Therefore, the security of any nuclear power plant is directly related to national energy security.²³² On the other hand, the radiation risks to workers, the public, and the environment must be assessed, and physical security must be given high priority.

The security of the nuclear installations is first of all the responsibility of the owner of the facility, and then it comes under the banner of national security. If the security of the installations is not fully ensured, then national security is directly affected and there

²²⁹ Beril Tugrul, Selahattin Çimen, “Assessment of Sustainable Energy Development, Energy Systems and Management” Springer, Chapter 10, Heidelberg, 2015, pp. 109-114.

²³⁰ TAEA, Decree on Licensing of Nuclear Installations No: 18256, 1983.

²³¹ TAEA, ibid.

²³² Beril Tugrul, “Contemporary Strategies for Energy Supply Security”, *International Conference on Military and Security Studies (ICMSS-2015)*, Istanbul, Proceeding-pp. 126-130.

may be undesirable consequences. In addition, the risks may transcend national borders, and international cooperation serves to promote and enhance overall security.

In order to construct and operate a nuclear installation, it is to obtain a license from the Authority. Therefore, the applicant must submit an application to the Authority, enclosing documents detailing the nature of the installation to be constructed and describing the technical and financial capacity of the implementer.²³³ International inspection by the International Atomic Energy Agency (IAEA) is required for all nuclear installation due to the Nuclear Non-Proliferation Treaty (NPT) agreement.

States have an obligation of diligence and duty of care, and are expected to fulfil their national undertakings and obligations; this is also required under international regulations. International security standards provide support for States in meeting their obligations under general principles of international law, such as those relating to environmental protection. Therefore, a national nuclear security regime is in place and is being continuously improved for all countries having nuclear installations. National security infrastructures are fundamental to this concept.

Security policies are aimed at protecting human life, health and the environment in addition to the security of the installation itself. Accordingly, security procedures must be designed and implemented in an integrated manner to ensure security at all levels. The security of nuclear installations, nuclear material and sources of radiation are essential to safety and the failure of any procedures entail consequences for nuclear safety.²³⁴

It is important to ensure that health, environmental, security, quality and economic requirements are not considered separately from security requirements. The exclusion zone, i.e. the controlled area in the vicinity of the nuclear installation, is of paramount importance within the management system, overriding all other concerns.

The organization shall be able to demonstrate the effective fulfilment of its management system requirements. The management system shall identify and integrate with the requirements with the national security. Security procedures and standards constitute a useful tool for contracting parties to assess their performance under these concepts. Therefore, “nuclear security is fundamental in the management of nuclear technologies and in applications where nuclear or other radioactive material is used or transported.”²³⁵

²³³ TAEA, *ibid.*

²³⁴ IAEA, “The Management System for Nuclear Installations”, *IAEA Safety Standards Series*, No. GS-G-3.5, Vienna, 2009.

²³⁵ IAEA, “Computer Security at Nuclear Facilities”, *IAEA Nuclear Security Series*, No. 17, Technical Guidance - Reference Manual, 2011.

Cyber Security

Information Communication Technologies (ICT) range from small personal computers and computerized equipment to national assets. Critical infrastructure is growing day by day around the world. Along with the widespread use of ICT, cyber risks have also been rising at an unpredictable rate.²³⁶

There are many definitions of cyber security. One of the accepted definitions is “Information Assurance”, defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation.²³⁷

Computer security plays an increasingly vital role in ensuring the security of nuclear installations. It will address the establishment and improvement of programs to protect those computer systems, networks and other digital systems that are critical for the safe and secure operation of the facility and for preventing theft, sabotage and other malicious acts. Along with the widespread use of computer systems, cyber risks have been rising at a significant rate. In this complex and expanding cyber environment, we now face a problem in regard to how institutions will manage to protect themselves against cyber threats.

Cyber security encompasses different disciplines. All of these disciplines should be involved in cyber security activities. These are:

- Personnel security;
- Physical security;
- Information security;
- Computer security.

All disciplines of security (including personnel, physical, information and computer) interact and complement each other to establish a facility’s security posture. Figure 1 shows the relation among these disciplines. A failure in any of the disciplines of security could impact the other domains and cause extra requirements on the remaining aspects of security.²³⁸

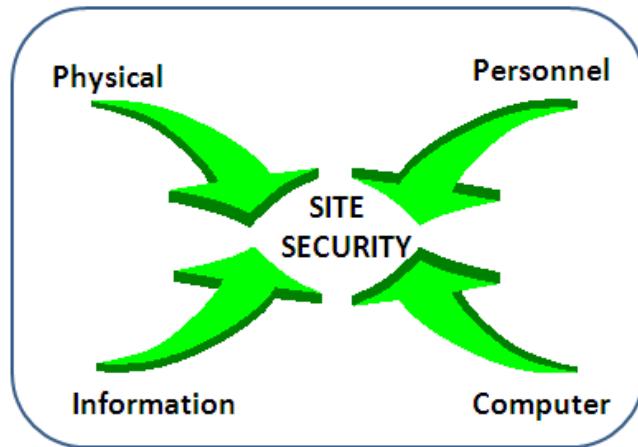
²³⁶ Muharrem Karaman, Hayrettin Catalkaya, “Institutional Cyber Security: A Case Study of Open Source

Intelligence and Social Networks”, International Conference on Military and Security, 2015.

²³⁷ CNSS, 2010, National Information Assurance Glossary, Committee on National Security Systems. Instruction CNSSI-4009 dated 26 April 2010.

²³⁸ IAEA, ibid.

Figure 1. Interaction among the Cyber Disciplines



Current trends in advanced systems show huge demands on computers and communication. As a result, Information Technology (IT) infrastructure is one of the main components of cyber security, especially for control systems. Control systems are based on integration and interoperability.

A nuclear installation is supported by a networking system, which makes it a huge and strategic target. Therefore, there is more scope for attacking the systems. This requires system designers to take extra care in protecting against unwanted attacks on IT systems, in order to make the whole system resistant to hackers.²³⁹

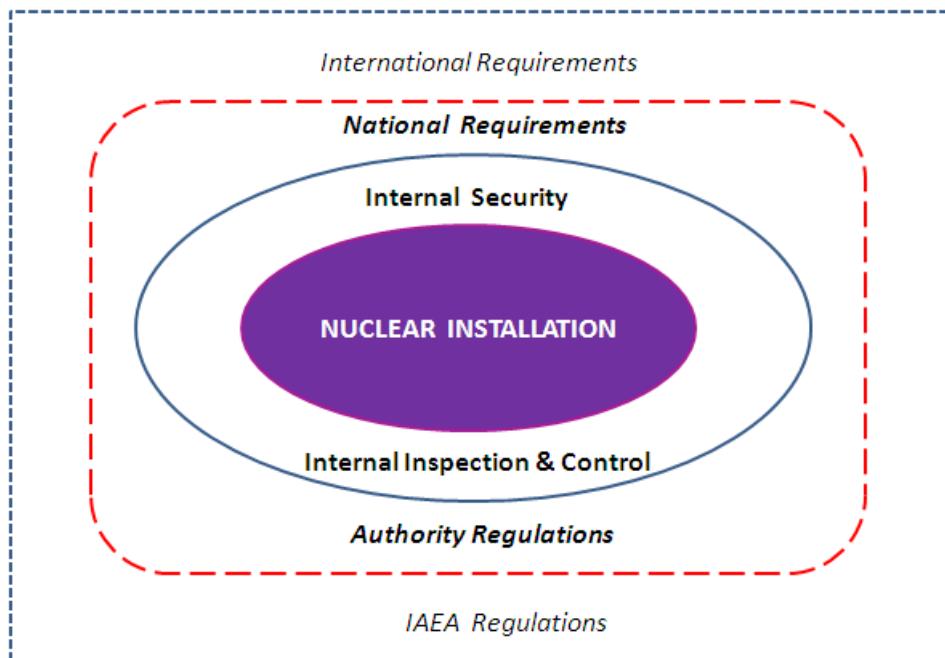
In reality, many activities at nuclear facilities are controlled by management systems.²⁴⁰ Security, safety, health, environmental, quality and economic elements are integrated within a single management tool or a set of integrated and mutually reinforcing systems with cyber security.²⁴¹ Cyber security is relevant to almost all facility activities.

²³⁹ Ömer Dogan, Kerem Mustafa Koşaner, International Conference on Military and Security Studies (ICMSS-2015), Istanbul, Proceeding, pp. 26-31.

²⁴⁰ IAEA, The Management System for Facilities and Activities, IAEA Safety Standards Series No, GS-R-3, Vienna, 2002.

²⁴¹ IAEA, op. cit.

Figure 2. Requirements for a Nuclear Installation



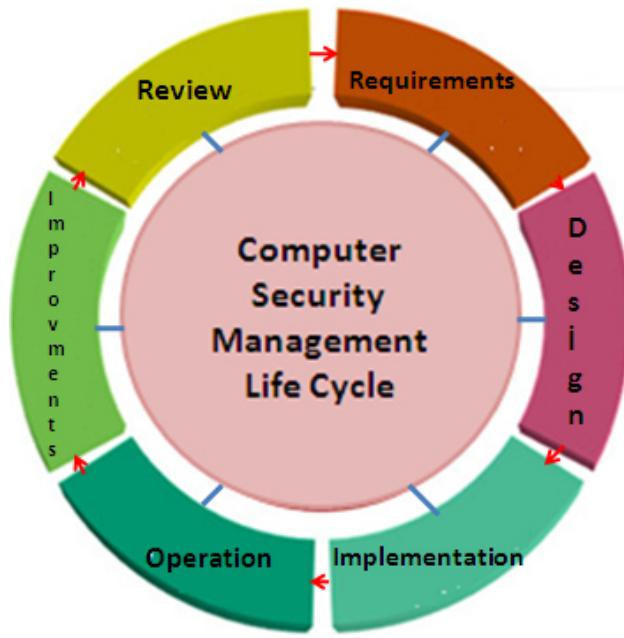
As seen in Figure 2, there are numerous requirements, regulations, decrees, and guidelines for a nuclear installation in regard to designing the facility management system. Furthermore, there are multiple levels of standards, including institutional, national and international. This complex interplay of standards can be highly complicated, but the management system must be able to cope with these requirements.

1. Provision of Cyber Security

Computer security is extremely important for all stages during the establishment of nuclear installations.²⁴² Therefore, computer security is important at each stage for nuclear installations from construction to management and from qualifying to decommissioning. This is known as the “Computer Security Management Life Cycle”, as shown in Figure 3 below.

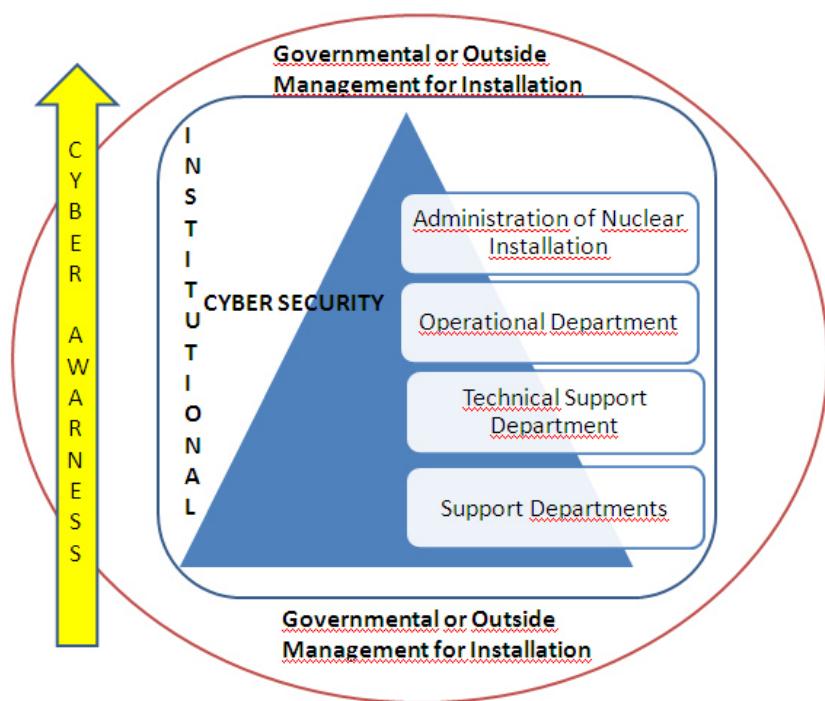
²⁴² IAEA, *ibid.*

Figure 3. Computer Security Management Life Cycle



Computer security requires administrative, technical and operational management. It also includes a number of supporting procedures. The main element of cyber security organization (shown in Figure 4) is always in close connection with government or outside management. Therefore institutional cyber security, which is also valid for governmental entities, must be handled systematically and thoroughly.

Figure 4. Cyber Security Organization



Cyber security is of paramount importance and it should be based on the “defense in depth” concept. Defense in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would all have to fail or be defeated before a computer system could be compromised. If one level of protection or barrier were to fail, a subsequent or barrier would be in place.²⁴³ In order to provide effective protection, the function of “Computer Security Officer” may be assigned to the “IT Security Officer” or “Information Security Officer”. It may also be shared among multiple people.

2. Protection of Cyber Security

Cyber security is important in every dimension for nuclear installations. Successful protection of computer systems may be achieved by adapting best practices and tools developed within the wider computer security community, while also taking into account the specificities of the nuclear industry.

Some of the main components of cyber security for nuclear installations include:

- Cyber Strategy, Policies and Roadmap
- Defining the Cyber Environment and Operational Design
- Cyber Security, Situational Awareness and Education
- Risk Assessment, Standardization, Cyber Resiliency
- Secure System Architecture
- Vulnerability Assessment
- Central Incident Management
- Log Management and Correlation
- Continuous Monitoring and Auditing
- Business Continuity

Any computer network or information system is vulnerable to two types of attacks, passive and active.

Passive attacks can include traffic analysis and the release of internal or external communications. Unfortunately, passive attacks are generally very difficult to detect. Designers should consider this threat during the design phase, for instance by using encryption techniques.²⁴⁴ Active attacks involve the modification of data streams or the creation of false streams.

Conclusion

The nature and range of threats to security and also cyber security have become extremely complex and unpredictable, but remain of vital importance for the nuclear sector. It is also important to remember that no security system is foolproof.

²⁴³ IAEA, ibid.

²⁴⁴ Ömer Doğan, Kerem Mustafa Koşaner, ibid.

Nuclear installations should be communicating with their institutional, governmental and related associations quickly and reliably. Many cyber risks can be avoided through effective protection systems.

Appropriate security mechanisms are used to detect, prevent or recover from a security attack. There are many security mechanisms that help to detect a cyber attack. These include digital signatures, access control, data integrity, authentication exchange, traffic padding, routing control, notarization, trusted functionality, security label, event detection, auditing, and recovery.²⁴⁵

In order to ensure sustainable institutional cyber security, the following steps should be taken:

- Control and check the cyber systems frequently;
- Procedural processes should be examined to consist of the usage of social networks among personnel;
- Information that reveals the institution's organizational structure (e.g. operational or logistics departments) or users' credentials should not be used in the names of computer, server or related equipment. Instead simple names and numbers should be used;
- Vulnerability tests and security auditing should be conducted periodically;
- Risk assessment documents, including new and emerging cyber threats must be updated according to international standards and virtualization technologies should be used in networks;
- All nuclear facilities should establish their own Cyber Incidents Response Teams (CIRT);
- At the administrative and technical levels, social networks should consider confidentiality, integrity, and availability of information including employee privacy.

All nuclear installations should have a cyber security policy, endorsed and enforced by the management system using the life cycle concept. The policy specifies the overall cyber security goals of the installations based on institutional and national security requirements. This study analyzes the complexity, components, and importance of cyber security for nuclear facilities, pointing out some of the essential cyber security processes.

²⁴⁵ Ömer Doğan, Kerem Mustafa Koşaner, ibid.

REFERENCES

CNSS, National Information Assurance Glossary, Committee on National Security Systems. Instruction CNSSI-4009 dated 26 April 2010.

DOGAN, O., KOŞANER, K.M., International Conference on Military and Security Studies (ICMSS-2015), Istanbul.

IAEA, The Management System for Facilities and Activities, IAEA Safety Standards Series No, GS-R-3, Vienna, 2002.

IAEA, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No.GS-G-3.1, 2006.

IAEA, The Management System for Nuclear Installations, IAEA Safety Standard Series No. GS-G-3.5, Vienna, 2009.

IAEA, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, Technical Guidance - Reference Manual, 2011.

KARAMAN, M., CATALKAYA, H., Institutional Cyber Security: A Case Study of Open Source Intelligence and Social Networks, International Conference on Military and Security Studies (ICMSS-2015), Istanbul, Proceeding, 2015.

ŞİŞANEKİ, I., Akin, O., KARAMAN, M., SAGLAM M., "A Novel Concept for Cyber Security: Institutional Cyber Security", 6th International Conference on Information Security and Cryptology, Turkey, Ankara, Sep. 20-21, 2013.

TAEA, Decree on Licensing of Nuclear Installations No: 18256, 1983.

TUGRUL, A. B., "Energy Policy and Interactions with Politics and Economics", International Conference on Energy Environmental Engineering - ICEEE 2014, 21-22 November 2014, Paris-France, Proceeding, 2014.

TUGRUL, A. B., Cimen, S., Assessment of Sustainable Energy Development, Energy Systems and Management Springer, Chapter 10, Heidelberg, 2015.

TUGRUL, A. B., "Decision Making Process in Energy Policies", Yıldız Technical University-YTU, Political Science and International Relations-PSIR Bulletin, No: 11, 2015.

TUGRUL, A. B., Contemporary Strategies for Energy Supply Security, International Conference on Military and Security Studies (ICMSS-2015), Istanbul, Proceeding, 2015.

CIP SECURITY AWARENESS AND TRAINING: STANDARDS AND PRACTICE

Rafał LESZCZYNA

ABSTRACT

These are critical infrastructure employees who have access to the critical cyber assets in the first place. This situation is well recognized by international and national standardization bodies which recommend security education, training and awareness as one of the key elements of critical infrastructure protection. In this chapter the standards are identified and their relevant areas are described. A practical implementation of the recommendations by means of a university course is presented.

Key Words: CIP, Training, Awareness, People Factor, Education

Introduction

Security experts agree that people are the critical factor in protection of the organization's cyber assets. The end-users access the assets on a regular basis and in most cases either they lack the security knowledge necessary to protect them or they know how to avoid protection mechanisms – in both cases the result is the same, namely the exposure of the cyber assets to threats.²⁴⁶

At the same time the majority of organizations concentrate their information security budget on technical solutions. This is because technical methods are well-defined (thus – comprehensible) and give an illusion that when applied all security issues will be solved. Acquire a “box” – an anti-virus, a firewall or an anti-malware – install it, and consider the problem solved.²⁴⁷

This approach tends however to be ineffective. Surveys show that despite the gradually increasing investments in technical controls the number of intrusions reported annually also continues to rise. Interestingly, there are reports claiming that the majority of breaches were caused by insiders. Technical solutions cannot make a network more

²⁴⁶ Stephanie D. Hight, “The Importance of a Security, Education, Training and Awareness Program,” 2005.

²⁴⁷ Motorola, “The User Role in Information Security,” 2010.

secure than activities of people who use it, because poor user practices overcome even the most carefully planned security system.²⁴⁸

Educating and raising security awareness among personnel is like expanding the information security department into the whole organization. Instead of few security experts trying to protect the network, security manager has at his/her support each employee of the organization taking care of the security interests of the company. This establishes some sort of a “human firewall” that will be very likely more efficient than a technical solution, and in contrast to it, able to recognize unknown, previously undetected threats.²⁴⁹

The importance of Security Education, Training and Awareness (SETA) is today widely recognized in the cybersecurity domain. The relevant security requirements and controls are described in majority if not all of security standards. The number of SETA initiatives continues to grow.²⁵⁰

In this chapter security requirements and controls in the standards most relevant to Critical Infrastructure Protection (CIP) are presented, followed by a description of a case study: teaching information security management (including CIP) at technical university in Poland.

Definitions

Security awareness is defined as set of activities that promote security, establish accountability, and provide personnel with updated information on threats, vulnerabilities, security solutions and so on.²⁵¹ It should result in that any individual who has access to the organization’s information assets is aware of potential consequences and his/her responsibilities.

Information security training aims at developing relevant security knowledge and skills within the workforce. It supports competency evolvement and aids personnel in understanding and learning how to perform their security functions. The most important difference between training and awareness is that the objective of training is to teach skills that allow a person to perform a specific role, while awareness aims at focusing an individual’s attention on a certain issue.²⁵²

Role-based training provides security courses that are adjusted to the particular needs of any group of people with significant responsibilities for information security in their organization.²⁵³

²⁴⁸ Motorola, *ibid*.

²⁴⁹ Motorola, *ibid*.

²⁵⁰ Stephanie D. Hight, *ibid*.

²⁵¹ Pauline Bowen, Joan Hash, Mark Wilson, “NIST SP 800-100 Information Security Handbook: A Guide for Managers.” Gaithersburg, USA, 2006.

²⁵² Pauline Bowen, Joan Hash, Mark Wilson, *Ibid*.

²⁵³ Pauline Bowen, Joan Hash, Mark Wilson, *Ibid*.

Security education aims at creating specialists and professionals capable of designing new security solutions and acting proactively. It integrates security skills and competencies from various functional areas and extends it with a multidisciplinary study of concepts, issues, and principles (technological and social). It is delivered as part of higher education.²⁵⁴

Critical Energy Infrastructure Standards: The Role of Education and Awareness Raising

Critical Infrastructures

Critical infrastructures consist of the physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.²⁵⁵

In European Union a critical infrastructure is defined as an '*asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*'.²⁵⁶

The American definition of the term refers to '*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*'.²⁵⁷

²⁵⁴ Pauline Bowen, Joan Hash, Mark Wilson, Ibid.

²⁵⁵ Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism (COM(2004) 702 final).

²⁵⁶ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

²⁵⁷ USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), section 1016(e).

Table 1. Critical infrastructure sectors depending on the classification

Critical infrastructure sectors	
European classification²⁵⁸	American Classification²⁵⁹
Energy installations and networks	Chemical
Communications and information technology	Commercial Facilities
Finance (banking, securities and investment)	Communications
Health care	Critical Manufacturing
Food	Dams
Water (dams, storage, treatment and networks)	Defense Industrial Base
Transport (airports, ports, intermodal facilities, railway and mass transit networks and traffic control systems)	Emergency Services
Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)	Energy
Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)	Financial Services
	Food and Agriculture
	Government Facilities
	Healthcare and Public Health
	Information Technology
	Nuclear Reactors, Materials, and Waste
	Transportation Systems
	Water and Wastewater Systems

From various sectors recognized as critical (see e.g. two classifications in Table 1) the energy and transport are depicted as of the highest priority.²⁶⁰

²⁵⁸ COM(2004) 702 final.

²⁵⁹ Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience.

²⁶⁰ Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/0786 final).

Critical Energy Infrastructures Cyber Security Standards

The number of standards and guidelines which to a greater or lesser extent refer to the cybersecurity of critical energy infrastructures is fairly high, which results in the situation that sometimes it is difficult to orientate oneself in this plethora of publications.

ENCS STUDY

Addressing this challenge, in 2013-2014 the European Network for Cyber Security (ENCS) conducted a study which aimed at the identification of standards which are the most relevant to the security of smart grids and smart grid Distribution Service Operators (DSOs).

The study, based on the previous investigations of various institutions (e.g. CEN, CENELEC, ETSI, ENISA, etc.) resulted in the identification of 11 publications enlisted in

Table 2.

Table 2. CIP energy cybersecurity standards

Publication	Type	No. of occurrences in the studies
IEC 62351	Standard	5
NERC CIP	Regulation	4
IEC 62443 (ISA 99)	Standards and guidelines	4
IEEE 1686-2007	Standard	4
ISO/IEC 27001	Standard	3
NISTIR 7628	Guideline (Technical Report)	3
NIST SP 800-53	Guideline (Special Publication)	3
IEC 62357	Technical Report	2
ISO/IEC 27002	Standard	2
NIST SP 800-82	Guideline (Special Publication)	2

ENISA Studies

Critical infrastructures, such as electricity generation plants, transportation systems, oil refineries, chemical factories and manufacturing facilities are large, distributed complexes. The majority of them uses Industrial Control Systems (ICS) for monitoring and control. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems.

In 2011, the European Network and Information Security Agency (ENISA) conducted a study in the domain of ICS and SCADA. Its objective was to obtain the view on the ICS protection primarily in Europe but also in the international context. The study based on the previous work done in the ESCoRTS project, and specifically on “D2.1 - Survey of Existing Methods, Procedures and Guidelines” recognized around international or significant national standards and guidelines dedicated to ICS. The study was followed in 2012 in reference to Smart Grids and resulted in the identification of further ICS standards and guidelines. The results of both studies are presented in Table 3.

Table 3. Standards and guidelines dedicated to industrial control systems identified in the ENISA studies

Standards and guidelines dedicated to industrial control systems	
IEC 62351. Data and communications security	IEEE 1686-2007. Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
IEC 62210. Power system control and associated communications - Data and communication security	IEEE 1402. Guide for Electric Power Substation Physical and Electronic Security
IEC 62443. Security for Industrial Process Measurement and Control: Network and System Security	IEEE 1711. Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
Security Profile for Advanced Metering Infrastructure	ISO 27000
ISO/IEC 15408, Evaluation criteria for IT security (also known as “Common Criteria”)	ISA 99. Manufacturing and Control System Security

Cyber Security Assessments of Industrial Control Systems. A good practice guide	Configuring & managing remote access for industrial control systems. A good practice guide
Good practice guide - Process Control and SCADA Security	Firewall deployment for SCADA and process control networks. A good practice guide
Process Control Domain (PCD) – Security Requirements for Vendors	NAMUR NA 115. IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries
VDI/VDE 2182 Series	OLF Guideline No. 104. Information security baseline requirements for process control, safety and support ICT systems
OLF Guideline No. 110. Implementation of information security in Process Control, Safety and Support ICT Systems during the engineering, procurement and commissioning phases	CheckIT
CRIOP	Guide to Increased Security in Industrial Control Systems
NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security	NIST SP 800-53. Recommended Security Controls for Federal Information Systems
NISTIR 7176. System Protection Profile - Industrial Control Systems	Field Device Protection Profile for SCADA Systems in Medium Robustness Environments
AGA Report No. 12. Cryptographic Protection of SCADA Communications	API 1164, Pipeline SCADA Security
API Security Guidelines for the Petroleum Industry	21 Steps to Improve Cyber Security for SCADA Systems
Catalogue of Control Systems Security: Recommendations for Standards Developers	Securing your SCADA and Industrial Control Systems

ICS Standards

The standards address various aspects of security of industrial controls systems: data and communication security, security requirements and controls, risk management, security programs and other issues.

For instance, IEC 62351 and IEEE 1711 focus on data and communication security. IEC 62351 introduces security measures to protocols used in the energy sector, such as IEC 60870-5 (DNP3, IEC101, IEC104) or IEC 60870 (TASSE.2/ICCP). IEEE 1711 defines a cryptographic protocol to provide integrity and optional confidentiality for cyber security of serial links.²⁶¹

NERC CIP, DHS Catalogue of Control Systems Security, NIST SP 800-53, ISO/IEC 27001 or ISA/IEC 62443²⁶² are industry-recognized standards which describe security requirements and controls which are essential for building a security framework in a system as they explicitly define security measures which must be present in the system in order to assure its protection.

Knowing the controls and requirements, operators can request specific security functions from vendors in the products they offer. They can also consider appropriate criteria when making purchasing decisions. For instance, IEEE 1686-2007 defines the functions and features to be provided in substation IEDs to accommodate Critical Infrastructure Protection (CIP) programs. Another example are “WIB Security Requirements for Vendors”, which provide requirements and recommendations for IT security to be fulfilled by vendors of process control and automation systems.²⁶³

Another group of publications is devoted to risk management related concepts and methodologies, and includes, for example, ISA-62443-3-2, or NISTIR 7628, which is based on NIST SP 800-39, NIST SP 800-30, FIPS 200, FIPS 199, NERC Vulnerability and Risk Assessment and other documents.

For an enterprise, a very important aspect of cyber security is to establish an Information Security Management System (ISMS). There are very few documents which advise operators on how to incorporate industrial control systems into their ISMS. One of them is IEC 62443-2-1, which adapts the relevant content of ANSI/ISA 99, defines the elements necessary to establish a cyber security management system (CSMS) for ICS and provides guidance on how to develop those elements. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

²⁶¹ ENISA, “Protecting Industrial Control Systems - Recommendations for Europe and Member States”, ENISA, 2011.

²⁶² ENISA, Ibid.

²⁶³ ENISA, Ibid.

Other documents that help operators develop such an ISMS system are API 1164 or a combination of the famous ISO/IEC 27000 framework with NIST SP 800-82. API 1164 provides pipeline SCADA operators with a description of industry practices in SCADA security, and a framework needed to develop sound security practices within the operator's individual companies.

ISO/IEC 27000 framework is composed of information security standards which provide recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS). The series is broad in scope and non-ICS-specific, aiming at organizations of all structures and sizes. For this reason it is necessary to use it in conjunction with other, more specific publication(s), for example NIST SP 800-82.

NIST SP 800-82 provides guidance on securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. The document gives an overview of ICS and typical system topologies, identifies common threats and vulnerabilities and provides recommended security countermeasures to mitigate the associated risks. It also addresses specific security controls for ICS, provides enhancements to classic ones and a supplemental guidance for the controls which can be applied in a practically straightforward manner. NIST 800-82 is well recognized among the ICS users, providers and supporters (public bodies, standardization bodies, academia and R&D).²⁶⁴

Preliminary Cyber Security Framework

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity. The framework aims at supporting critical infrastructure owners and operators in reducing cybersecurity risks in industries such as power generation, transportation and telecommunications. It relies on a variety of existing standards, guidelines, and practices and indicates them adequately to each area of critical infrastructure protection in the Framework Core. These references include publications such as: ISO/IEC 27001, NIST SP 800-53, ISA 62443, COBIT and CCS.

Cyber Security Education, Training and Awareness Raising in the Standards

Practically all standards which are not strictly technical but address higher level cybersecurity issues, such as security management or administration, underline the importance of actions related to education or training or awareness raising of users.

In this chapter we present the requirements or controls in the most relevant standards (see

Table 2).

²⁶⁴ ENISA, Ibid.

NERC CIP

NERC CIP-004-3 requires that all personnel (including contractors and service vendors) authorized to access critical cyber assets have an appropriate level of training and security awareness.

For this purpose a security awareness program must be implemented which includes security awareness reinforcement on at least quarterly basis using mechanisms such as:

- Direct communications (e.g., e-mails, memos, computer based training, etc.)
- Indirect communications (e.g., posters, intranet, brochures, etc.)
- Management support and reinforcement (e.g., presentations, meetings, etc.)

The awareness program should go hand in hand with a cyber security training program, reviewed and updated at minimum on annual basis. This program will ensure that all relevant personnel is trained before they are granted access to critical cyber assets and covers at minimum:

- The proper use of critical cyber assets
- Physical and electronic access controls to the assets
- The proper handling of asset information
- Action plans and procedures to recover from a cyber security incident

ISO/IEC 27001 and 27002

In ISO/IEC 27001, the A.8.2.2 security control ("Information security awareness, education and training") imposes that all employees of an organization, contractors and third party users receive awareness training and regular updates in organizational policies and procedures relevantly to their job function.

ISO/IEC 27002 provides additional guidance on the implementation of the control. Awareness training should start with a formal introduction of the organization's security policies and expectations. This must be done yet before access to critical information assets or services is granted. Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process.

The aim of the awareness raising activities is to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role. They must include information on known threats, contact person and the proper channels for reporting information security incidents.

ISA 99

In ISA-62443-2-1-WD the security control 8.2.2 (“Security awareness, education, and training”) is specified which identically as in the 8.2.2 control from ISO/IEC 27001²⁶⁵ requires that all relevant users receive awareness training and regular updates in organizational policies and procedures relevantly to their job function. **“This should include the information necessary to identify, review, address and where appropriate, remediate vulnerabilities and threats to Industrial Automation and Control Systems (IACS).”**

The standard provides implementation guidance and control enhancements **including the IACS-specific guidance**. The latest, among the others, imposes that IACS operators and maintenance staff should participate in the training.

Awareness training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of IACS facilities and information on the disciplinary process. A formal introduction of the organization’s security policies and expectations must be given before granting the users the access to information or the IACS.

The security awareness, education, and training activities must be tailored to the skills and the role of a user and should include information on known threats and vulnerabilities, a contact person for further security advice and reporting channels for security incidents. All personnel must be instructed about social engineering techniques.

According to IEC/TR 62443-3-1, as part of a personnel security program, all employees, contractors, or temporary workers should be completely trained in their basic job responsibilities, the terms and conditions of their employment, disciplinary actions and appeal process, security requirements, and safety requirements. Each employee should be reviewed periodically and/or retraining must be settled down to ensure that employees remain aware of their job functions.

NIST IR 7828

The NIST IR publication recognizes security awareness as a critical part of information system incident prevention and dedicates to it the SG.AT (Awareness and Training) family of controls.

It requires from organizations:

- Designing effective training programs based on individuals’ roles and responsibilities
- Developing, establishing and maintaining awareness and training security policy
- Performing basic security awareness briefings to all Smart Grid information system users

²⁶⁵ ISA 99 is partially based on ISO/IEC 27001.

- Providing security-related training first before authorizing access to the information system or performing assigned duties and after that – periodically or induced by a substantial change
- Maintaining a record of awareness and training for each user
- Establishing and maintaining contact with security groups and associations to share security-related information including threats, vulnerabilities, and incidents and to be informed about the newest recommended security practices, techniques, and technologies

NIST SP 800-53

NIST Special Publication 800-53 in the family AT “Awareness and Training” defines four controls which impose:

1. The development, documentation and dissemination of security awareness and training policy and procedures
2. Training of information system users (including managers, senior executives, and contractors) as part of initial training for new users and periodically thereafter
3. Provision of role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the information system or performing assigned duties and periodically thereafter
4. Documentation and monitoring of individual information system security training activities and retention of individual training records

For each control, supplemental guidance is provided as well as control enhancements when needed.

Besides the AT family, there are several controls defined in other families which refer to security education, awareness and training.

PM-13 “Information security workforce” requires the establishment of an information security workforce development and improvement program.

PM-14 “Testing, training, and monitoring” ensures that an organization provides and coordinates security testing, training, and monitoring activities. These activities must be informed by current threat and vulnerability assessments.

CP-3 “Contingency training” and IR-2 “Incident response training” impose the provision of contingency and incident response trainings.

SA-16 “Developer-provided training” ensures that (external or internal) developer of the information system, system component, or information system service to provide training on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

NIST SP 800-82

According to NIST SP 800-82: "Many of the interconnections between corporate networks and ICS require the integration of systems with different communications standards. (...) Because of the complexity of integrating disparate systems, control engineers often fail to address the added burden of accounting for security risks. Many control engineers have little if any training in security and often IT security personnel are not involved in ICS security design. As a result, access controls designed to protect control systems from unauthorized access through corporate networks are usually minimal."

The quasi standard recognizes security awareness as a critical part of ICS incident prevention, in particular in reference to social engineering. Thus it recommends providing training and raising security awareness as part of security program development. The training and awareness activities will facilitate the implementation of an ICS security program as they prepare the employees for changes resulting from it. They also demonstrate management's commitment to a cyber security program. Feedback from personnel participating in the training can be a valuable source of information for improving the security program.

NIST SP 800-82 security controls for awareness and training direct a reader to the Awareness and Training family from NIST SP 800-53 in the first place. Additionally the following publications are indicated:

- NIST SP 800-12 – for guidance on security policies and procedures
- NIST SP 800-16 – for guidance on security training requirements
- NIST SP 800-50 – for guidance on security awareness training
- NIST SP 800-100 – for guidance on information security governance and planning

NIST SP 800-82 provides an ICS specific recommendations and guidance on security awareness and training, which among the others, imposes the inclusion of control system-specific information for specific ICS applications into the awareness and training program as well as the need of training of all personnel having significant ICS roles and responsibilities. The program must cover the physical process being controlled as well as the ICS.

Case Study: Teaching Information Security Management at Technical University

Recognizing the importance of security awareness in enterprises and organizations especially those which belong to critical infrastructures, the information security management course was introduced in 2010 into the curriculum of students of the Faculty of Management and Economics at Gdańsk University of Technology. The aim of the course is to introduce a student with the fundamentals and key concepts of information security management, with a particular attention to the security management lifecycle. The formula of the course is conceptualized in the way that

during laboratory exercises students, working in groups, pass the subsequent phases of the lifecycle, starting from choosing an enterprise which will undergo the phases and concluding with designing adequate security controls (whether technical, administrative or physical). The laboratory work is accompanied with a lecture which aims at introducing the relevant knowledge beforehand. There are fifteen hours of lecture and thirty hours of lab in a semester.

Lecture

The contents of the lecture are as follows:

- Introduction: the context of information security, knowledge based economy, the growth of number and complexity of attacks, problems and challenges, critical infrastructures, NIST and ISO, legal requirements, definitions of basic security terms
- Cost of the information security management in an enterprise: rationale, key premises of management decision, scarcity of security cost assessment methods, brief review of existing methods
- Information Security Management System (ISMS): explanation, lifecycle
- Standard ISO/IEC 27001: key characteristics, ISMS, PDCA model, detailed explanation of the four phases of the ISMS lifecycle, Annex A – control objectives and security controls, example-based explanation of a security control
- NIST Special Publication 800-53: NIST document types (standards, special publications, others), NIST partners and consultants, NIST SP 800-53 objectives, security controls, example-based explanation of a security control, baseline controls, risk management framework, FIPS 199 and 200
- Information security management process in accordance with ISO/IEC 27001 and NIST SP 800-53
- Information security policy
- Security threats: descriptions and taxonomies
- Risk management: introduction, basic concepts (risk, threat, vulnerability etc.), frameworks and standards, lifecycle, risk analysis methods, detailed explanation of the simplified qualitative risk assessment method
- Technical security controls: firewalls, cryptography, identification and authentication, access control, intrusion detection systems
- Physical security, personnel security, information security awareness and training

During the lecture the importance of securing critical infrastructures is explained and several vivid examples of scenarios of attacking the infrastructures are presented including Stuxnet, Flame or a fictional attack on the U.S. Nation's Critical Infrastructure.

Lab

The lab work constitutes the core of the security management course. The lessons go in parallel to the lecture, but their contents are postponed to the lecture, so the students are introduced to each subject. This is possible, because in the first stage, students need to form groups and each of the groups must choose an existent enterprise or propose a fictitious one, for which they will perform all further analyses. Then the enterprise needs to be analyzed from the security point of view, so among the others to facilitate assessments of threat impact. Thus the business model and functioning of the enterprise must be analyzed in the first place, as depending on it, some information assets are more and some less important. Students describe the mission, goal, organizational structure and the main activities of the organization. Then they analyze the information system of the organization, describe it and prepare diagrams. All results are compiled into a report. This introductory part takes three weeks (2 hours a week). In the meantime, the students listen to the lecture about concepts necessary for the performance of further studies (cost assessment in that case).

During the next two weeks, students assess the cost of information security management in the enterprise. To do so, they determine values of a set of parameters characterizing the enterprise, such as the number of users, number of security professionals or hire rate. Based on the data, cost estimations are obtained. Students analyze the results and present the conclusions and the related data in a report.

Risk assessment constitutes the subsequent part of the lab exercises. Students identify all information assets in their organization, describe them and assess the impact of violating confidentiality, integrity and availability of these assets. Each student group analyses available security threat lists and taxonomies and prepare the list of threats adequate to their company. Then for six selected, according to a justified criterion, information assets, the students evaluate threat probabilities and assess risks. As for each part of the lab work, students consolidate the results into a report.

When students are aware of the security context of their organization, know the possible threats, their impact on the company business, and are able to systematize information assets based on the associated risks – they can prepare information security policy. The resulting policy document should be the outcome of the analysis of other available publications as well as effects of previous work.

The lab concludes with selecting security controls in accordance with the standard chosen between ISO/IEC 27001 and NIST SP 800-53. Students justify their choice of the standard and select the security controls for the six information assets selected during the risk assessment. They describe the controls and if applicable – present the control areas not addressed by the controls. Each group prepares the new diagram of the information system which incorporates technical security solutions. Finally the students describe their conclusions and observations.

To complete the course, students must participate in all five parts of the laboratory with adequate results and well written report. Besides, they need to pass the knowledge assessment which is based on open questions as well as multiple choice test. The questions include those which refer to critical infrastructures. For instance in the most recent edition of the course students had to explain the notion of critical infrastructure and indicate which attack discovered in 2010 targeted among the others Iranian nuclear facilities.

Conclusion

Recognizing the crucial role of users in Critical Infrastructure Protection, the cybersecurity standards used in the energy sector, such as NERC CIP, ISO/IEC 27001, ISA 99 or NIST SP 800-82, recommend designing and establishing Security, Education, Training and Awareness Programs (SETA), which define SETA policies, roles and responsibilities. The latest include direct and indirect communications or management reinforcement to bring the employees' attention to security issues (awareness raising), teaching specific security-related skills (training) or more long-term and multidisciplinary studies usually performed at universities (education).

The experiences from delivering an information security management course at Faculty of Management and Economics of Gdańsk University of Technology show the key role of practice in the education of information security. Assessments demonstrate that students more willingly refer to the knowledge and experiences obtained during lab exercises than the theoretical knowledge received from the lecture. With a course designed as a combination of lab work and a lecture, with the focus on the former, it is possible to achieve positive results of the assessments, indicating that students have sufficient level of information security awareness.

The information security management course was introduced to the curricula of students of management and economics because many of graduates will later take managerial and administrative positions in enterprises and organizations, and on their decisions will depend the cybersecurity condition in their companies. For this reason such a fundamental cybersecurity course should be provided in all academic institutions of a similar profile. The introduction of the course should be also discussed to the technical faculties linked to the infrastructures identified as critical, for example electrical and control engineering faculties or chemistry faculties.

REFERENCES

BOWEN, P., HASH, J., WILSON, M., "NIST SP 800-100 Information Security Handbook: A Guide for Managers", Gaithersburg, USA, 2006.

Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism (COM (2004) 702 final.

ENISA, "Protecting Industrial Control Systems - Recommendations for Europe and Member States", 2011.

Motorola, "The User Role in Information Security", 2010.

Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience.

USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), section 1016(e).

HIGHT, S. D., "The Importance of a Security, Education, Training and Awareness Program," 2005.

CYBER SECURITY EDUCATION AND TRAINING FOR CRITICAL INFRASTRUCTURE PROTECTION

Dr William HURST

Dr Nathan SHONE

Carl CHALMERS

ABSTRACT

The level of critical infrastructure technology has been steadily transforming over the last decade in order to keep pace with the growing demand for the services offered. The implementation of the smart grid, which relies on a complex and intelligent level of interconnectivity, is one example of how vital amenity provision is being developed. However, with these changes, the risk of threats from the digital domain must be calculated. Superior interconnectivity between infrastructures means that the future cascading impacts of successful cyber attacks are unknown. As such, Critical Infrastructure Protection (CIP) is becoming more essential than ever before. Cyber attacks have the potential to cause a critical infrastructure outage and the subsequent impact on a network of such infrastructures is yet unknown. Education, training and awareness now have important roles in the future fight against cyber crime.

Key Words: Critical Infrastructure, Cyber Security, Smart Grid, Critical Infrastructure Protection Training

Introduction

Cyber crime is given considerable publicity globally; with increasing digital threats having a worldwide economic bearing, reaching into the billions.²⁶⁶ In the United Kingdom, cyber threats are ranked as one of the top four risks to nationwide security, which is higher than that of a nuclear attack. In May 2015, the BBC reported on the fears posed by cyber attacks and how, specifically, critical infrastructures are in

²⁶⁶ E. Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security”, 2011.

danger.²⁶⁷ A single disruption can result in life-threatening consequences; critical infrastructure protection (CIP) now has a prominent role in national security matters.²⁶⁸ Additionally, with the growth in e-government services, the need for both the fortification of defense mechanisms and improved cyber threat awareness is evident and increasing year by year.

A continually evolving global ICT situation has seen new and more refined cyber threats arise. The emerging threats of Distributed Denial of Service Attacks caused by Botnets, in particular, and the destructive capabilities of cyber warfare, enforce the need to develop a well-rounded level of critical infrastructure resilience beyond the existing deficiency. Furthermore, remote reconnaissance is easier and more anonymous than ever before and political control can also be enforced through the Internet with communication governance.

Critical infrastructures, in particular, present a tempting target for terrorists, military strikes and hackers wanting to cause disruption, steal information or incapacitate a country remotely. The ability to attack a critical infrastructure from a distant location provides a previously unavailable way of conducting warfare, with the potential to cause more damage than a physical attack could. With this ability, incapacitating a country or causing harm to the population can be done without the victim knowing the exact origin of the attack.

In response, different governmental approaches are taken to tackle the issue. For example, in the European Union, the emphasis is on prevention and resilience. The aim is to develop a community and a “stronger together” approach to combat the growing cyber threat. The various types of initiatives set up by the EU all have the goal of improving international co-operation and the facilitation of communication between member states.

If member states do not work together, then they could, in fact, add to the risk to cascading failure through a lack of interoperability and understanding of how CIP works in other countries. In light of this, a holistic approach to critical infrastructure security is at the heart of EU’s efforts to increase the level of resilience and respond to growing levels of sophisticated cyber attacks.

In addition to the risk to critical infrastructures, cyber crime also has major impacts upon local communities. Cyber bullying on social networks, organized digital crime, identity theft and the exchange of illicit images are some of the many digital threats that the security forces have to contend with on a daily basis. With crimes, such as cyber harassment, hacked email accounts and phishing attacks particularly well

²⁶⁷ Dave Lee and Nick Kwek, “North Korean hackers ‘could kill’, warns key defector, BBC Technology News Online, <http://www.bbc.co.uk/news/technology-32925495>, (Accessed on June 2015).

²⁶⁸ Jennifer Betts and Şakir Sezer, “Ethics and Privacy in National Security and Critical Infrastructure Protection”, *Proceedings of IEEE International Symposium on Ethics in Science, Technology and Engineering*, 2014, pp. 1–7.

documented, local communities are working hard to combat the effects through the improved training of police high-tech crime units.

In light of the above issues, one of the main challenges for governments around the globe concerns the improvement of awareness for citizens and businesses about the threats existing in cyberspace. Often, organizations fail to address the issue of cyber security due to the costs involved in implementing a security system or training their staff in security measures. However, it is estimated by Lloyd's bank that the yearly mean cost to a company is currently \$400 billion worldwide.²⁶⁹ The estimated bill to an individual company is over \$2.1 million on average.²⁷⁰

Despite the publicity and real presence of the danger, there is a clear lack of awareness about cyber threats. Education and training for CIP should be on the forefront in the fight against the growing digital threat. Just as cyber defense systems must evolve, in order to counter the growing level of cyber attack sophistication,²⁷¹ so too should the level of cyber threat education advance. Training the next generation of cyber security experts and promoting the need for modernized security systems to be in place, is imperative.

Background

The arrival of new information technologies has resulted in different types of criminal activities, which previously did not exist. Each has the potential to cause extensive damage to internal markets.²⁷² Given the fact that the Internet does not have any boundaries, it makes it difficult to identify where attacks originate from and to counter them. For this reason, it is essential to promote education, awareness and international co-operation, in order to prevent cyber crime from being successful and growing exponentially.

A mindfulness of existing threats can play a role in preventative measures. For example, many people do not feel the need to use anti-virus software or take effective steps to protect their computing devices or personal data. This is potentially due to lack of knowledge about real threats and their impacts. The main problem with this is that malware can spread throughout the Internet and remain in circulation for long periods

²⁶⁹ Stephen Gandel, "Lloyd's CEO: Cyber attacks cost companies \$400 billion every year", <http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>, (Accessed on June 2015).

²⁷⁰ Alan Tovey, "Average cost of cyber attacks doubles to £1.46m", Telegraph Financial News Online,

<http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/11646347/Average-cost-of-cyber-attacks-doubles-to-1.46m.html>, (Accessed on June 2015).

²⁷¹ Christophe Feltus, Moussa Ouedraogo, Djamel Khadraoui, "Towards Cyber Security Protection of Critical Infrastructures by Generating Security Policy for SCADA systems", *Proceedings of the 1st International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2014, pp. 1–8.

²⁷² Lorcan Coyle, Mike Hinckey, Bashar Nuseibeh, Jose Luiz Fiadeiro, "Guest Editors' Introduction: Evolving Critical Systems", Computer (Long Beach Calif.), Vol. 43, No. 5, May 2010, pp. 28–33.

of time. In order to progress with the improvement of CIP, and counter the impacts of cyber crime in the local community, awareness is essential; as is an understanding of the needs to secure Internet-capable devices.

In addition, an attentiveness of the existing threats helps to develop a common understanding of the problems being faced.²⁷³ Awareness of the growing threat is one way of ensuring that protection measures are increased. If small and medium businesses and the general population, for example, have an increased consciousness of growing threats, more progress can be made on preventing the spread on Internet-based cyber threats.

1. Awareness Issues

There are, however, several challenging factors surrounding the improvement of cyber threat awareness. Firstly, the communication between the private and public sectors is often fairly poor. A large number of critical infrastructures are private sector owned. As the private sector is concerned about security risks, there is an unwillingness to disclose any information which could give competitors a financial advantage. In consequence, knowledge of cyber threats and their potential impacts is often not freely shared.

Secondly, one of the main awareness issues facing the security of critical infrastructures, in particular, is the integration of web-facing interfaces into key control devices, meaning they can be accessed from anywhere. Devices are connected online for a variety of reasons, particularly due to infrastructures being dispersed over wide geographic areas. This enables remote connection and control, saving on cost. The result is; engineers do not necessarily have to be dispersed to solve a problem, but instead can monitor the infrastructure from a central control location, which houses a control system. However, often critical infrastructure owners have little realization concerning the security of devices connected remotely.

In addition, security experts are starting to uncover safety issues and backdoors in the software used. Traditionally, SCADA and other control systems were part of closed networks which required an attacker to have physical presence inside the infrastructure in order to cause damage. As a result, one of the most commonly used control system software, SCADA (Supervisory Data Control and Acquisition), is now known to have specific cyber-weaknesses and was not designed with this much of security in mind. They present tempting targets for attack; as damaging the control software can influence the capabilities and service production.

Thirdly, a misplaced trust in existing security systems shows an awareness issue of the level of prevention methods in place and how effective they are. Infrastructures are

²⁷³ Thomas Mc Donogh, "Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure", Prof. Off. J. Eur. Union, Vol. COM(2009), No. 149 final, 2010.

protected through an in-depth defense approach. Different technology is used on each layer of the infrastructure to ensure that if an attacker penetrates one layer, they are not automatically able to access the next one. As a result, critical infrastructures are often described as having a harder outer shell with a ‘softer’ internal system, in terms of security. However, each of the layers of security provided through, either multiple Intrusion Detection Systems (IDS) or Unified Threat Management Systems (UTM), are known to have vulnerabilities which can be exploited through zero-day attacks.

Fourthly, on a community level, spear-phishing attacks are used for cyber crime purposes to disclose passwords, account details and ascertain payment details. Phishing attacks are becoming increasingly commonplace, and one specific type of phishing attack is known as a spear-phishing attack. This involves a targeted form of a phishing attack,²⁷⁴ where the success rate of the attack is higher compared with the generic bulk approach often used. Spear-phishing attacks are designed with a specific target in mind and rely on human error and a lack of threat awareness to be successful. Their aim is to trick the victim into thinking an email-based scam is legitimate by ensuring that the information inside is specific to that person or organization.²⁷⁵

As a result of successful spear-phishing attacks, numerous military and private industry systems have been breached; and each penetration is the direct result of lack of understanding about the nature of the attack, which leads to sensitive information being disclosed. In light of this, there is a clear need to enhance the level of cyber threat knowledge in general, for the profit of CIP. Specifically, the greatest benefit of increased awareness is a consciousness of existing vulnerabilities; thus eliminating the human weakness element through better education opportunities.

Finally, as an increasing level of cyber attack sophistication emerges, there needs to be an awareness of any potential future impacts. In the UK, for example, the rail industry is going through a modernization process, which has the goal of creating an automated railway system.²⁷⁶ The ambition is to optimize the performance of the network and enhance the way in which maintenance is carried out. Similarly, around the globe, the implementation of the smart grid is a further example of the movement towards introducing new innovations to enhance service provision. Its implementation is replacing traditional power distribution networks and creating a more intelligent

²⁷⁴ Mahmoud Khonji, Youssef Iraqi, and Andrew Jones, “Mitigation of Spear Phishing Attacks: A Content-based Authorship Identification Framework”, *Proceedings of the 6th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2011, pp. 416–421.

²⁷⁵ Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H. Raghav Rao, “Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email”, *IEEE Transactions on Professional Communication*, Vol. 55, No. 4, 2012, pp. 345–362.

²⁷⁶ Isidro Durazo Cardenas, Andrew Starr, Antonios Tsourdos, Maurizio Bevilacqua, and J. Morineau, “Precise Vehicle Location as a Fundamental Parameter for Intelligent Self-aware Rail-track Maintenance Systems”, *Proceedings of the 3rd International Conference in Through-life Engineering Services*, Vol. 22, 2014, pp. 219–224.

system, where functionality is intertwined with critical infrastructures, such as nuclear power plants. The way in which electricity is generated and distributed is revolutionized by its introduction.²⁷⁷ For example, the dynamic pricing for customers, distribution management advancements and demand management are all features which are brought about by this innovation.

Both are examples of critical infrastructures that are currently undergoing digital enhancement changes. The risk is that, unless awareness and general cyber security education is improved, technological improvements, such as these, will have significant cyber weaknesses which can be exploited, with potentially life-threatening consequences. Subsequently, the following section presents a case study on smart grids, as a future technology, and the surrounding cyber threat implications. Specific awareness issues and future risks are highlighted as part of the study.

2. Future Technology Case Study

A smart grid is a complex modern electricity system, which is able to automate the generation, distribution and consumption of electricity throughout the entire grid infrastructure. This is achieved through its vast sensor and monitoring capabilities, with each layer and component networked and completely automated at all levels. It provides a two-way flow of not only energy but also critical information and data to all of the grid stakeholders in real-time. This will fundamentally change the way in which we generate, distribute and monitor our electricity.²⁷⁸ The smart grid is essential for the integration of both renewable and more traditional energy resources; replacing the traditional top-down generation model of the current grid. It advances the efficiency and sustainability of electricity grids by its ability to self-heal, resist attack, and increase power quality and reliability.²⁷⁹ Smart grids are widely seen as the solution for providing the world with reliable electricity and meeting future increases in demand.

There are many social and customer benefits associated with the smart grid, including lower costs, improved customer service, decreased outage time and increased reliability, to name but a few.²⁸⁰ The smart grid actively encourages and enables consumer involvement and is a key part in ensuring its future success.²⁸¹ Allowing

²⁷⁷ Melike Erol-Kantarci and Hussein T. Mouftah, "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues", *IEEE Commun. Surv. Tutorials*, Vol. 17, No. 1, 2015, pp. 179–197.

²⁷⁸ Eric Knapp and Joel Broad, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems", Syngress, Elsevier, 2011.

²⁷⁹ National Energy Technology Laboratory, "A Systems View of the Modern Grid", https://www.smartgrid.gov/sites/default/files/pdfs/a_systems_view_of_the_modern_grid.pdf (Accessed on June 2015.)

²⁸⁰ Michael Anderson, "Social Benefits of the Smart Grid", ESNA, <http://www.esna.org/uploads/2010-06%3B%20Societal%20Benefits.pdf>, (Accessed on June 2015).

²⁸¹ Anna Mengolini and Julija Vasiljevska, "The Social Dimension of Smart Grids", *JRC Scientific and Policy Reports*, 2013.

consumers to monitor their electricity usage in real-time allows for informed decisions on how and when they consume their electricity.

One of the most important and fundamental components of the smart grid is the introduction of the Advanced Metering Infrastructure (AMI). The AMI offers bi-directional communication between the consumer and the rest of the smart grid stakeholders. This infrastructure removes the need for energy usage readings to be collected manually.²⁸² There are a number of features associated with the AMI, which enhance the level of CIP in place for the smart grid network. They include increased fraud detection, support for real-time pricing and improved fraud detection. The AMI can be broken down into three main areas: The Home Area Network (HAN), Wide Area Network (WAN) and the utility companies. The HAN is housed inside the consumers' premises and is made up of a collection of devices. The in-home display unit (IHD) is the most visible and accessible part of the AMI. It provides the consumer with up-to-date information on electricity usage, as well as the units of energy being consumed. Secondly, the smart meter provides real-time energy usage to both the consumer and all of the stakeholders. This builds detailed energy usage profiles of its consumers. Smart appliances also react to peak events within the smart grid ecosystem. Adapting to these events enables a reduction in demand on the grid and energy costs for the consumer.

One of the key components that reside in the AMI is the Smart Meter; they are seen as the foundation of any future smart electricity grid.²⁸³ The smart meter device will provide real-time energy usage to both the consumer and all of the smart grid stakeholders. Smart meters will be able to store 13 months of data keeping a record of total energy consumption. This allows the provider to build detailed energy usage profiles of its consumers. A smart meter has the built-in ability to disconnect-reconnect certain loads remotely and can be used to monitor and control the users' devices and appliances to manage demands and loads.²⁸⁴ These features enable for better grid management and control.

In general, organizations and utility companies have access to the data produced for analysis purposes; enabling them to have detailed and accurate information. This improves management and planning of activities. In addition, grid reliance and performance is enhanced, as demand can be better provisioned. It is, however, also a clear future security risk. If an attacker is able to gain access to the highly granular datasets about individuals, simple profiling techniques can be used to outline users'

²⁸² Mircea Popa, "Data Collecting from Smart Meters in an Advanced Metering Infrastructure", *Proceedings of 15th International Conference on Intelligent Engineering Systems*, pp. 137-142, 2011.

²⁸³ Andres Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin, "Private Memoirs of a Smart Meter", *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010, pp. 61–66.

²⁸⁴ Hassan Farhangi, "The Path of the Smart Grid", *IEEE Power Energy Magazine*, Vol. 8, No. 1, 2010.

behavior and ascertain information on their daily activities.²⁸⁵ This can, for example, be used to assess periods of the day when their house is unoccupied. Additionally, the key aspect about smart meters is that they have a remote off-switch, which is controlled by the service provider. If a way is found to successfully attack and shut down the devices remotely, then essentially every electronic device in a country can be stopped through one action.²⁸⁶

Thusly, it is clear from the introduction of new critical infrastructure technologies, such as the smart grid, that there is a need for ensuring effective educational practices are in place for the future protection. There is a real lack of awareness of the implications of a cyber attack. Training up the next generation of cyber security experts and improving the general level of awareness of existing threats is essential, especially as new intelligent technologies are put in place. In the following section, a discussion is put forward on CIP training and education.

CIP Training and Education

Critical infrastructure systems are undergoing one of the most significant computing-related adaptations, by moving from offline operational systems to fully interconnected online systems. This convergence between operational systems and information systems has raised numerous concerns; such as the aforementioned awareness issues, the need for cyber security for SCADA systems and the future security risks.

However, there is currently a global cyber security skills gap, and its continuing expansion is a major concern. A recent report found that 70% of UK enterprises outsource at least some of their security requirements due to lack of internal skills, despite an inherent reluctance to do so.²⁸⁷ This trending skills gap is showing no signs of relenting; by 2017 it is estimated that there will be a shortage of 2 million professionals²⁸⁸ in the UK alone. When combined with the increasing number of high-profile cyber attacks, this raises concerns regarding the protection of national critical infrastructure systems.

The field of CIP is inherently complex, as it combines several different disciplines such as cyber security, data management, information technology, operations management, physical security, and safety management. Additionally, there is a diverse range of industrial sectors that are considered as ‘critical infrastructures’, such as finance, transport, power, water, waste, manufacturing, chemical, communications and

²⁸⁵ Carl Chalmers, William Hurst, Michael Mackay, Paul Fergus, “Profiling Users in the Smart Grid”, *Proceedings of the Seventh International Conference on Emerging Networks and Systems Intelligence*, 2015.

²⁸⁶ Ross Anderson and Shailendra Fuloria, “Who Controls the Off Switch?”, *Proceedings of the First IEEE International Conference on Smart Grid Communications*, 2010, pp. 96–101.

²⁸⁷ Pierre Audoin, “Is Cyber Security Now too Hard for Enterprises?”, Cyber security trends in the UK, Fujitsu, 2015.

²⁸⁸ (ISC)2, Critical Times Demand Critical Skills, “An Analysis of the Skills Gap in Information Security”, *White Paper: Booz Allen Hamilton Strategy and Technology Consultants*, 2013.

emergency services. Each has their own set of objectives, potential consequences and attitudes towards security. Trying to confluence the CIP training needs, contents and objectives from both operational and cyber security perspectives is a difficult task. Additionally, the diversity of the roles within each organization and sector requires a high complexity to integrate up-to-date topics and content that is specific and relevant to each role. As a result, there is a great deal of disparity within current CIP training programs and certification schemes, as raised by the recent ENISA report.²⁸⁹

1. Training Environments

CIP is predominantly a knowledge-driven subject with a high degree of practical application, making it a difficult subject to teach using traditional methods (e.g. lectures and literature), which are largely theoretical. This difficulty is due to learners being unable to apply theoretical knowledge in a practical real-world scenario. This is a point emphasized by Willems *et al.* who detail that “the trainee cannot apply the principles from the academic approach to a realistic environment”.²⁹⁰ Therefore, training institutions are required to provide suitable practical training environments for learners to practice their skills, the implementation of which can pose significant difficulties.

The importance of practical skills was emphasized in the 2015 ENISA report, which found that 75% of survey respondents identified that practical skills are essential criteria that make certification credible.²⁹¹ There are, however, many different types of practical environments that can be used for CIP training.

One common implementation strategy is the physical lab. Some institutions are able to offer training, using genuine CI hardware and software. This is the best form of training, as it will provide learners with exact replications of the real-world infrastructure and hardware they will be protecting. However, this approach is unfeasible for most, as the equipment is highly expensive to buy, manage and maintain. The use of physical hardware severely limits the number of users that can be trained at one time. The training also becomes highly specialized (i.e. targeting a specific industry or specific models of hardware), which therefore limits the scope of its appeal. Additionally, physical hardware rapidly becomes outdated, which means it is highly expensive to keep courses up-to-date; and this overhead cost is therefore passed on to the learners.

²⁸⁹ ENISA, “Certification Schemes at European Level for Cyber Security Skills of ICS/SCADA”, <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals>, (Accessed on June 2015).

²⁹⁰ Christian Willems, Thomas Klingbeil, Lukas Radvilavicius, Antanas Ceny and Christoph Meinel, “A Distributed Virtual Laboratory Architecture for Cybersecurity Training”, *Proceedings of the Int. Conf. Internet Technol. Secur. Trans*, 2011, pp. 408–415.

²⁹¹ ENISA, “Certification Schemes at European Level for Cyber Security Skills of ICS/SCADA”, <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals>, (Accessed on June 2015).

Secondly, simulation software offers the ability to learn in the virtual environment. Typically CI systems, particularly SCADA/ICS are closed source, meaning that the underlying software components are publically unavailable, including for training purposes. One mitigation strategy for this problem is the use of simulation, which allows trainers to create software representations of CI systems, with accurate modelling of behavioral characteristics and responses. This provides a more affordable, scalable and functional solution, which offers a high level of realism.

The main limitation with software simulations is that they are not a true representation of a real-world system. This pseudo-realism offered by simulators is often highly dependent upon its configuration. Simulations are also inherently limited, as they provide a standardized approach, however, each real-world system is uniquely configured and the occurrence of particular threats will not always produce the same behavior. They also do not consider many of the issues surrounding CIP, including the complex relationships that exist between components, as well as the social side of security (e.g. insider threats, disgruntled employees etc.). Although, there are many different simulation solutions, none can cover all of the specific machinery used at individual establishments. Therefore, applying the knowledge gained through CIP training can sometimes be a difficult task.

The creation of simulated CI testbeds is a trending area of research, with non-security specific approaches being developed such as those proposed by Farooqui *et al.*²⁹² and Dayal *et al.*²⁹³ as well as the seCPSim project.²⁹⁴ There are also many simulation-based training solutions that are targeted towards cyber security, although these are not CI-specific, they can offer more general security training. Some of the existing proposed solutions include Robo-Teacher²⁹⁵ which is a cyber security simulation-based educational system, LOST,²⁹⁶ a cyber security learning platform, and a cyber security training framework proposed by Fyte.²⁹⁷ There are currently several

²⁹² Adnan A Farooqui, Syed Sajjad Haider Zaidi, Attaullah Y Memon, and Sameer Qazi, "Cyber Security Backdrop: A SCADA Testbed", *Proceedings of the Computing, Communications and IT Applications Conference (ComComAp)*, 2014, pp. 98 – 103.

²⁹³ Avik Dayal, Ahmad Tbaileh, Yi Deng, Sandeep Shukla, "Distributed VSCADA: An Integrated Heterogeneous Framework for Power System Utility Security Modeling and Simulation", *Proceedings of the Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MCPES)*, 2015, pp 1–6.

²⁹⁴ Ceeman Vellaithurai, Anurag Srivastava, Saman Zonouz, "SECPSIM: A Training Simulator for Cyber-Power Infrastructure Security", *Proceedings of the IEEE SmartGridComm*, 2013, pp.61–66.

²⁹⁵ Bin Zhang, Kamran Shafi, and Hussein. A. Abbass, "Robo-Teacher: A Computational Simulation Based Educational System to Improve Cyber Security", *Adv. Intell. Syst. Comput.*, 2013, Vol. 208, 2013, pp. 179–186.

²⁹⁶ Jaume Abella, Guiomar Corral, Agustin Zaballos, "LOST Project, a Learning platform for Security Training", *Proceedings of the International Symposium on Computers in Education*, 2013, pp. 1–6.

²⁹⁷ Bryan K. Fyte, "Simulating Cyber Operations: A Cyber Security Training Framework", *Sans Institute*, <http://www.sans.org/reading-room/whitepapers/bestprac/simulating-cyber-operations-cyber-security-training-framework-34510>, (Accessed on June 2015).

commercial systems available, including Wombat Security Education Platform,²⁹⁸ Cybx²⁹⁹ and DETERLab.³⁰⁰

Thirdly, the introduction of virtualization and hypervisor technologies in a virtual lab environment has drastically increased the accessibility of cyber security training in particular. This has launched a new wave of training environments that allow mass simulations from a single machine and do not affect the realism or credibility of the system. The use of virtualized training environments is highly efficient, particularly for real environments that are too expensive to replicate, for example SCADA systems. This technology has given rise to a number of new CI-orientated cyber security environments, such as those proposed by Morris *et al.*³⁰¹ and the EU-funded SCADA LAB.³⁰² There have also been several proposed virtualized platforms for more generic cyber security training (which could easily be applied to certain CI environments), such as the Tele-Lab project³⁰³, Ameen and Ahmed's proposed e-laboratory³⁰⁴ and CYDEST.³⁰⁵

Finally, training and education can be offered through a hybrid approach. There are some recent research projects that are combining both physical hardware and simulation software. This allows for greater levels of realism (e.g. supporting genuine

²⁹⁸ Wombat Security," Security Awareness Training Platform", <https://www.wombatsecurity.com/security-education>, (Accessed on June 2015).

²⁹⁹ Cybx "Security Training Courses", Cybx, <http://www.cybx.org/services/training-courses/>, (Accessed on June 2015).

³⁰⁰ DeterLab, "DETERLab Education Site", <https://education.deterlab.net/>, (Accessed on June 2015).

³⁰¹ Thomas Morris, Rayford Vaughn, and Yoginder Dandass, "A testbed for SCADA Control System Cybersecurity Research and Pedagogy", *Proceedings of the Seventh Annu. Work. Cyber Secur. Inf. Intell. Res CSIRW '11*, 2011.

³⁰² Antonio Sánchez Aragó, Enrique Redondo Martínez, and Sandra Salán Clares, "SCADA Laboratory and Test-bed as a Service for Critical Infrastructure Protection", *Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research*, 2014, pp. 25–29.

³⁰³ Christian Willems, Thomas Klingbeil, Lukas Radvilavicius, Antanas Ceny and Christoph Meinel, "A Distributed Virtual Laboratory Architecture for Cybersecurity Training", *Proceedings of the Int. Conf. Internet Technol. Secur. Trans*, 2011, pp. 408–415.

³⁰⁴ Siddeeq Y. Ameen and Ibraim M. Ahmed, "Design and Implementation of e-Laboratory for Information Security Training", *Proceedings of the Fourth Int. Conf. e-Learning*, 2013. pp. 310–317.

³⁰⁵ Stephen Bruecknera, David Guasparia , Frank Adelsteina , Joseph Weeks, "Automated Computer Forensics Training in a Virtualized Environment", *Digital Investigation*, Vol. 5, 2008, pp. 105–111.

CI protocols such as Modbus) but with improved upgradeability and reduced cost. Such approaches have been proposed by Morris *et al.*³⁰⁶ and Queiroz *et al.*³⁰⁷

The predominant problem with existing CIP training is the lack of specialism, as most training is generic and not tailored for specific roles and industries. CIP is a specific and specialized area, as CI implementations are mostly unique; therefore, the relevant training needs to be equally as specific.

2. Training Procedures

As CIP is a practical subject, there are many different training delivery methods that could be utilized within the environments detailed previously. Some of the most commonly utilized methods include war games, simulated breaches, and vulnerability identification.

Cyber warfare games (e.g. capture the flag) are used to provide learning opportunities that can simulate real-world cyber crises and professional attacks. This provides a safe environment for learners to gain first-hand experience of dealing with the conditions that arise. It also allows for the observation and monitoring of learners' performance in order to provide constructive feedback, which can help improve their knowledge, capabilities, understanding, and awareness. This delivery method allows learners to experience both attacking and defending CI networks. The knowledge of both how to attack and how to defend is equally valuable, particularly for high-value CI networks.

Simulated breaches/attacks allow for highly specific breaches or attacks to be replayed to learners, which may be unique to their role or sector. These types of simulation allow learners to experience and observe the symptoms and patterns of fundamental problems, in a controlled environment. This form of training is excellent for practicing real-time threat detection and prevention, as well as post-event forensic analysis.

Activities/challenges are essential tasks that learners must be able to conduct on operational systems. By practicing in a training environment, both simple and complex tasks that are either generic or specific to learners' roles can be safely rehearsed and perfected. This is the most common form of training delivery and is often referred to as tutorials.

Vulnerability identification includes problems that are deliberately created in a training environment, which are to be identified and resolved by learners. This provides essential experience in protecting CI networks by identifying potential weaknesses or

³⁰⁶ Thomas Morris, Rayford Vaughn, and Yoginder Dandass, "A testbed for SCADA Control System Cybersecurity Research and Pedagogy", *Proceedings of the Seventh Annu. Work. Cyber Secur. Inf. Intell. Res CSIRW '11*, 2011.

³⁰⁷ Carlos Queiroz, Abdun Mahmood, Jiankun Hu, Zahir Tari, Xinghuo Yu, "Building a SCADA Security Testbed", *Proceedings of the Third International Conference on Network and System Security*, 2009, pp. 357–364.

attacker entry points, and devising solutions to address them. Their efforts to secure the training environment will often be evaluated by using pen testing techniques.

3. Future Improvements

There are currently two emerging branches of pedagogical technology, which could soon be applied to improve the effectiveness of future CIP training. The first one is the use of intelligent tutoring, which provides individualized tutoring for learners. Using automated assessment rather than human feedback allows for more accurate, rapid and detailed prescriptive and proscriptive feedback for users to act upon.³⁰⁸ Intelligent tutoring allows for a deeper level of assessment of practical knowledge and understanding, e.g. determining the correctness of the steps taken to reach a result, rather than just the final result. Obviously, each CI implementation is different and as such practical assessment environments can be difficult to devise. Hence, there is already some ongoing research to develop a CI security assessment lab.³⁰⁹

The second improvement is the use of personalized learning, which offers learners with a learning environment uniquely constructed to suit them.³¹⁰ It allows for training courses to be tailored to meet specific requirements, as well as account for their existing strengths and weaknesses. Individual learning styles can be determined and learning pathways constructed,³¹¹ which provides a highly efficient and effective method of learning at their own pace. More importantly, it will allow generic CIP training to be tailored to suit individual roles or sections more easily. Personalized learning is currently a hot topic for research, focusing on theoretical or interactive learning, but the concept can easily be applied to more physical and practical environments.

Conclusion

As increasing demand is placed on critical infrastructures, their size and importance are growing every year. The implantation of new intelligent technologies has resulted in an increase in the number of remote access points into a critical infrastructure network; meaning they are more exposed and vulnerable than ever before.

Protecting these infrastructures is clearly a key issue. As threats increase, it becomes clear that security may lie away from conventional computer security techniques, and

³⁰⁸ David Boud, "Sustainable Assessment: Rethinking Assessment for the Learning Society", *Stud. Contin. Educ.*, Vol. 2, 2000, pp 151–167.

³⁰⁹ Guillermo A Francia, Noureddine Bekhouche, and Terry Marbut, "Design and Implementation of a Critical Infrastructure Security and Assessment Laboratory", *Proceedings of the 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing*, 2011, pp. 1–6.

³¹⁰ Antonio Garrido and Eva Onaindia, "Assembling Learning Objects for Personalized Learning: An AI Planning Perspective", *Proceedings of the IEEE Intelligent Systems*, 2013, pp. 64–73.

³¹¹ Norsham Idris, Norazah Yusof, and Puteh Saad, "Adaptive Course Sequencing for Personalization of Learning Path Using Neural Network", *Int. J. Adv. Soft Computer*, Vol. 1, No. 1, 2009, pp. 49–61.

an original approach to CIP will be required. Improving the level of support, increasing awareness and education of cyber security matters is key to the well-being of people and the evolution of critical infrastructure security levels. As threats evolve and become more adaptive, so should cyber security education measures adapt themselves to bridge the growing skills gap.

REFERENCES

- ABELLA, J. and CORRAL, G., ZABALLOS A., "LOST Project, a Learning platfOrm for Security Training", *Proceedings of the International Symposium on Computers in Education*, 2013.
- AMEEN, S. Y. and AHMED, I. M., "Design and Implementation of e-Laboratory for Information Security Training", *Proceedings of the Fourth Int. Conf. e-Learning*, 2013.
- ANDERSON, R. and FULORI, S., "Who Controls the Off Switch?", *Proceedings of the First IEEE International Conference on Smart Grid Communications*, 2010.
- ARAGÓ, A. S., MARTÍNEZ E. R., and CLARES S. S., "SCADA Laboratory and Test-bed as a Service for Critical Infrastructure Protection", *Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research*, 2014.
- BETTS, J., SEZER §., "Ethics and Privacy in National Security and Critical Infrastructure Protection", *Proceedings of IEEE International Symposium on Ethics in Science, Technology and Engineering*, 2014.
- BOUD, D., "Sustainable assessment: Rethinking Assessment for the Learning Society", *Stud. Contin. Educ.*, Vol. 2, 2000.
- BRUECKNERA, S., GUASPARIA, D., ADELSTEINA, F., WEEKS, J., "Automated Computer Forensics Training in a Virtualized Environment", *Digital Investigation*, Vol. 5, 2008.
- CARDENAS, I. D., STARR A., TSOURDOS A., BEVILACQUA, M., MORINEAU, J., "Precise Vehicle Location as a Fundamental Parameter for Intelligent Self-aware Rail-track Maintenance Systems", *Proceedings of the 3rd International Conference in Through-life Engineering Services*, Vol. 22, 2014.
- CHALMERS, C., HURST, W., MACKAY, M., FERGUS, P., "Profiling Users in the Smart Grid", *Proceedings of the Seventh International Conference on Emerging Networks and Systems Intelligence*, 2015.

COYLE, L., HINCHEY, M., NUSETIBEH B., FIADEIRO J. L., Guest Editors' Introduction: Evolving Critical Systems, Computer (Long. Beach. Calif), Vol. 43, No. 5, May 2010.

DAYAL, A., TBAILEH A., DENG and SHUKLA Y. S., "Distributed VSCADA: An Integrated Heterogeneous Framework for Power System Utility Security Modeling and Simulation", *Proceedings of the Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSPES)*, 2015.

EROL-KANTARCI M., MOUFTAH H. T., "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues", *IEEE Commun. Surv. Tutorials*, Vol. 17, No. 1, 2015.

FARHANGI, H., "The Path of the Smart Grid", *IEEE Power Energy Magazine*, Vol. 8, No. 1, 2010.

FAROOQUI A. A, ZAIDI S. S. H., MEMON A. Y, QAZI S., "Cyber Security Backdrop: A SCADA Testbed", *Proceedings of the Computing, Communications and IT Applications Conference (ComComAp)*, 2014.

FRANCIA G. A., BEKHOUCHE, N., MARBUT T., "Design and Implementation of a Critical Infrastructure Security and Assessment Laboratory", *Proceedings of the 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing*, 2011.

FYTE, B. K., "Simulating Cyber Operations: A Cyber Security Training Framework", *Sans Institute*, <http://www.sans.org/reading-room/whitepapers/bestprac/simulating-cyber-operations-cyber-security-training-framework-34510>, (Accessed on June 2015).

GANDEL S., "Lloyd's CEO: Cyber-Attacks Cost Companies \$400 Billion Every Year", <http://fortune.com/2015/01/23/cyber attack-insurance-lloyds>, (Accessed on June 2015).

GARRIDO A., ONAINDIA E., "Assembling Learning Objects for Personalized Learning: An AI Planning Perspective", *Proceedings of the IEEE Intelligent Systems*, 2013.

IDRIS N., YUSOF N., SAAD P., "Adaptive Course Sequencing for Personalization of Learning Path Using Neural Network", *Int. J. Adv. Soft Computer*, Vol. 1, No. 1, 2009.

(ISC)2, Critical Times Demand Critical Skills, "An Analysis of the Skills Gap in Information Security", *White Paper*, Booz Allen Hamilton Strategy and Technology Consultants, 2013.

LEE D., KWEK N., North Korean hackers 'could kill', warns key defector, BBC Technology News Online, <http://www.bbc.co.uk/news/technology-32925495>, (Accessed on June 2015).

KHONJI, M., IRAQI, Y., JONES, A., "Mitigation of Spear Phishing Attacks: A Content-based Authorship Identification Framework", *Proceedings of the 6th International Conference for Internet Technology and Secured Transactions* (ICITST, 2011).

MARKHAM, A. M., SHENOY, P., F., Kevin, CECCHET, E., IRWIN, D., "Private Memoirs of a Smart Meter", *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010.

MC DONOGH, T., Opinion of the European Economic and Social Committee on the "Communication from the Commission to the European Parliament", *The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure*, Prof, Off. J. Eur. Union, Vol. COM (2009), No. 149 final, 2010.

MENGOLINI, A., VASILJEVSKA, J., "The Social Dimension of Smart Grids", *JRC Scientific and Policy Reports*, 2013.

MORRIS T., VAUGHN R., DANDASS Y., "A Testbed for SCADA Control System Cyber Security Research and Pedagogy", *Proceedings of the Seventh Annu. Work. Cyber Secur. Inf. Intell. Res CSIIRW '11*, 2011.

QUEIROZ, C., MAHMOOD, A., HU, J., TARI, Z., YU X., "Building a SCADA Security Testbed", *Proceedings of the Third International Conference on Network and System Security*, 2009.

TOVAY, A., Average Cost of Cyber Attacks Doubles to £1.46m, Telegraph Financial News Online,
<http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/11646347/Average-cost-of-cyber-attacks-doubles-to-1.46m.html>, (Accessed on June 2015).

VELLAITHURAI C., SRIVASTAVA A., ZONOUZ S., "SECPSIM: A Training Simulator for Cyber-Power Infrastructure Security", *Proceedings of the IEEE SmartGridComm*, 2013.

WILLEMS C., KLINGBEIL T., RADVILAVICIUS L., CENY A., MEINEL C., "A Distributed Virtual Laboratory Architecture for Cybersecurity Training", *Proceedings of the Int. Conf. Internet Technol. Secur. Trans*, 2011.

ZHANG, B., SHAFI, K., ABBASS, H., A., "Robo-Teacher: A Computational Simulation Based Educational System to Improve Cyber Security", *Adv. Intell. Syst. Comput*, 2013, Vol. 208, 2013.

THE IMPORTANCE OF PUBLIC-PRIVATE PARTNERSHIPS IN CRITICAL INFRASTRUCTURE PROTECTION

David SUTTON

ABSTRACT

The loss of or curtailment to critical infrastructure (CI) sectors such as energy, water, communications, transport, health, finance, food, government and public safety, whether arising from man-made or natural incidents, has a profound impact both on individuals and on society as a whole. The interdependency between these CI sectors, especially energy, cannot be underestimated.

Following the 9/11 attacks in the United States, the UK's communications industry regulator and the government's Cabinet Office jointly instigated a Public-Private Partnership (PPP) of the electronic communications industry, the regulator and central government departments.

This paper describes the background to the PPP; its aims and objectives; how a trusted relationship developed between public and private sectors, particularly in cases where competing organizations needed to work together as a team; and how as a result of realistic scenario-based exercises the members responded successfully to real-world incidents including the July 2005 London bombing attacks.

Key words: Trust; information sharing; traffic light protocol; public-private partnership; interdependency; electronic communications

Introduction

The interdependency between areas of Critical Infrastructure (CI) is well understood, and the impact of failures is felt both by individuals and by society as a whole. When a major incident that affects any CI area occurs, response to and the management of the incident becomes the primary concern of the relevant emergency response teams.

With incidents in which there is less consequential impact on other areas of CI, the individual response teams may usually act successfully in isolation, but for those incidents that do have a major impact on other CI areas, it follows that there must be close communication between the wider response community. Many such incidents will require the contribution of both public and private sectors in order to bring about

successful resolution. The resulting organizations are referred to as Public-Private Partnerships (PPPs).

In the UK, the Centre for the Protection of National Infrastructure (CPNI) has defined the national infrastructure as “those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends”. It consists of the following nine areas³¹²:

- Communications;
- Emergency services;
- Energy;
- Financial services;
- Food;
- Government;
- Health;
- Transport;
- Water.

Whilst all are key to society, this paper primarily addresses the importance of public-private partnerships in the interdependency between electronic communications and energy – specifically in the supply and distribution of electricity.

From the electronic communications side, the story begins following the terrorist attacks on the New York's World Trade Center (WTC) in September 2001, as a result of which the network operator Verizon's Building at 140 West Street suffered severe damage from the collapse of the WTC1 and WTC7 buildings. As a consequence of the damage, Verizon lost 200,000 voice lines, 100,000 private branch exchange (PBX) lines, 4.4 million data circuits, and 11 cell sites. Over 14,000 business and 20,000 residential customers were affected.³¹³

In hindsight, it is clear that there would be a very significant impact on large-scale centralised telephone systems (whether fixed or mobile) and large concentrations of Internet connectivity (also known as peering points) following an incident that affected their premises. This would degrade and even inhibit the ability of both the general public and front-line emergency responders to communicate.

A key report³¹⁴ into the events of 9/11 listed three ‘guiding principles’ or criteria to identify and characterise the need for flexibility as it applies to infrastructure services. These are:

³¹² See <http://www.cpni.gov.uk/about/cni/>

³¹³ Thomas D. O'Rourke, Arthur J. Lembo, A and Linda K. Nozick, **Lessons Learned from the World Trade Centre Disaster about Critical Utility Systems**, (2003), Cornell University, p. 277.

³¹⁴ Rae Zimmerman, **Public Infrastructure Service Flexibility for Response and Recovery in the September 11 Attacks at the World Trade Center**, (2003), Institute for Civil Infrastructure Systems, Wagner Graduate School of Public Service, New York University, p. 243.

- the provision of alternative routes, facilities or locations to build new capacity or to redistribute existing capacity where services have been destroyed or substantially reduced as a consequence of an extreme event;
- the organisational capability and capacity needed, including knowledge of how those systems operate and the ability to control them in a crisis;
- the ability to share information about the state of the infrastructure and the alternatives available in a way that is easy to understand, in order to reduce the impact of a major infrastructure-related incident.

It is upon these guiding principles that successful PPPs are founded.

Interdependency between energy and electronic communications

It is worth taking a brief look at the nature of the interdependencies between energy and electronic communications in order to better understand the need for a PPP that is able to respond to major incidents.

If we begin by looking at the impact of failures of both infrastructures, it will be clear that the shorter the interruption to service, the less impact will be felt both by the service's wider customer base and more especially by the interdependent service.

The impact of failures in energy supply upon electronic communications networks

Thankfully, widespread failures of energy, especially across Western Europe are rare, but the consequences of a major outage – whatever its cause – can be extreme. As an example, the blackout in November 2006³¹⁵, when an incident in the North German electricity transmission area caused supply disruptions to more than 15 million households across Europe. The country most affected was France where 5 million customers were without power.

Whilst the core of electronic communications networks are designed to be highly resilient both to their own failures and failures of energy supply, this is not the case at the network end points, where equipment relying on local supply can fail immediately on power outage, or if provided with short-term battery backup may remain operational for a limited period of time.

In the higher order parts of their networks, electronic communications network operators normally provide uninterruptible power supplies, backed up by standby generation, but increasingly, customers rely on the local electricity supply to power landline wireless telephones and internet routers, making them highly susceptible to outages.

In the world of mobile communications, base stations are not usually backed up by standby generation, as this tends to be expensive to provide, operate and maintain,

³¹⁵ Antii Silvast and Joe Kaplinsky, **White Paper on Security of European Electricity Distribution**, (2007), UNDERSTAND research project funded by the European Union, p. 35.

and is generally used only in extreme cases such as remote areas where power supplies may be unreliable.

More recently, fixed-line and Internet service providers have delivered broadband data services through ‘Fibre to the Cabinet’ technology, which again requires continuous power in order to deliver service to the end user.

Fortunately, the majority of power supply interruptions are of short duration and are rectified either automatically by pre-defined actions within the electricity network, or by manual intervention by staff at network operations centres within the affected networks.

The impact of electronic communication failures upon energy networks

Looking at the other side of the coin, energy networks make heavy use of electronic communications in the transmission of status information from network components and locations back to regional and national monitoring and control centres; the transmission of commands to alter the configuration of key network components in the reverse direction; and the exchange of information, requests or instructions between those centres and the operational staff who may either have to report on network component status or carry out physical configuration changes in cases where automatic methods cannot be used.

However, if the wired or wireless networks used within the energy sector are not resilient on an end-to-end basis, the network control centres could lose visibility of the status of the network and would be unable to make changes, resulting in the risk of network collapse under extreme conditions such as the example above, or in cases of severe weather.

Initial PPP developments in the UK electronic communications sector

Following 9/11, the UK Regulator Oftel, took the view that whilst individual public fixed and mobile communications service providers would undoubtedly have their own response and recovery plans, their very interdependency (regardless of any further CI interdependencies) would require significant cooperation between them, and was concerned that there was no existing provision for this.

Oftel sought and received support from the government’s Cabinet Office to initiate a meeting of all the major UK public telecommunications providers in an attempt to find a way forward. This meeting took place in December 2001 in central London.

Fewer than a dozen private organizations were represented at this initial meeting, with attendees coming almost entirely from a network operations background. For the most part, there had rarely been a requirement before for them to meet their counterparts face-to-face, and therefore this unusual gathering was outside anybody’s sphere of experience. Once Oftel had explained the background and the rationale for the meeting, it became clear that the objective was to bring organizations together in order

to work for the common good, and the discussion changed quickly from “Why are we here?” to “How can we make this work?” This was the first vital step in bringing about the PPP.

By the meeting’s end, consensus was reached that each network service provider would report back to their senior management board recommending that a tripartite public-private partnership (PPP) should be formed, which would examine ways in which information could be shared between organizations, government departments and the regulator, and how mutual assistance might be undertaken in times of crisis.

Over the next few months, network service providers were able to take the first steps towards a nascent organisation known as the Telecoms Industry Emergency Planning Forum (TI-EPF) whose participants would:

- work together as a team without fear of competitive disadvantage;
- identify and evaluate the threats, vulnerabilities and potential impacts facing the UK’s electronic communications infrastructure;
- recommend and implement both short-term and longer-term solutions to improve resilience and mutual aid;
- produce plans to respond to major incidents and exercise those plans in order to verify their fitness for purpose.
- produce and exercise a mechanism for alerting all PPP members in the event of a CI-affecting incident in order to enable a timely and effective response.

The organisation initially consisted of a number of fixed and mobile public network service providers, Oftel (Chair), the Cabinet Office and the Department of Trade and Industry, the lead government department with responsibility for telecommunications.

The PPP’s members developed a Memorandum of Understanding (MoU), which had to be ratified by all the organizations at Board level. This took some months to achieve, but in the meantime the members began work developing the forum’s Terms of Reference³¹⁶ on the basis that the MoU would eventually be signed and that the spirit of working together was more important than the signed document.

Later development

In late 2003, Oftel was given wider powers and changed its name to Ofcom. As a result of the changes, it was felt that the regulator was not the most suitable leader for the forum, and the Chair transferred to the Cabinet Office for a period of time before finally becoming the responsibility of the private sector, rotating between member organizations. The organisation itself was also changing – growing in numbers and types of member organisation – and including the Internet community as well as the

³¹⁶ See

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62280/ec-rrg-terms-of-reference.pdf

conventional fixed and mobile voice organizations. It was realised that the PPP's title did not fully reflect the electronic communications industry as a whole, and it was subsequently changed to the Electronic Communications Resilience and Response Group (EC-RRG).

Over time, other organizations, both private and public joined the PPP, including the Centre for the Protection of National Infrastructure (CPNI), the Department for Communities and Local Government (DCLG), CERT-UK, the UK National Computer Emergency Response Team, representatives from the devolved administrations, and other 'qualifying' network operators, especially those in the Internet and broadcast services and Airwave³¹⁷. There are currently 20 private organizations in the PPP and 11 government/regulatory organizations.

The Department for Trade and Industry also changed its name, and is currently the Department for Business Innovation and Skills (BIS).

The overall structure of the EC-RRG is shown in Figure 1.

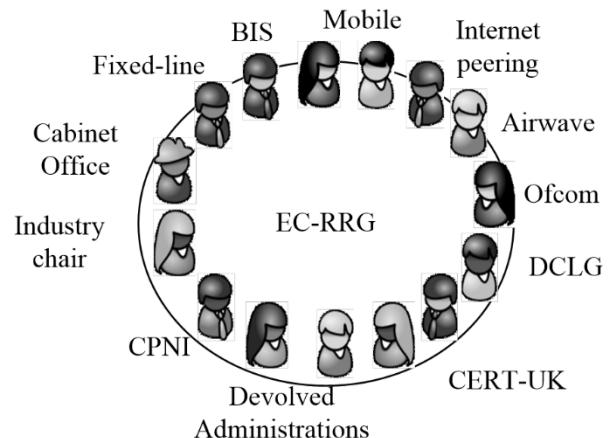


Figure 1 – The structure of the EC-RRG

The NEAT Process

One of the key aspects of the PPP's early work was the development of a method of alerting the forum's members in the event of an incident, and the process by which the subsequent incident would be managed. This was given the acronym 'NEAT' – the National Emergency Alert for Telecoms, and made provision for any member to request assistance from the forum by sending out an initial alerting message, requesting that members join a conference call in which the nature of the incident would be described and assistance requested. This conference call would normally be followed up as the incident progressed, and as other members were able to commit resources.

The NEAT process is tested regularly to ensure that member organizations are able to respond and to verify contact details, and the process has been used successfully on a number of occasions, notably on 7th July 2005 when the London bombings took place and the telecommunications networks initially suffered significant overloading, as will be discussed later.

³¹⁷ Airwave is the nation-wide mobile Terrestrial Trunked Radio (TETRA) network providing secure private communications for and between emergency responders and other accredited organizations. More information can be obtained from www.airwavesolutions.co.uk

Information sharing

Another important aspect of the PPP is that of sharing vital information between members in a manner that is:

- **Accurate** – hearsay and rumours may be interesting, but partners need to base decisions and plans on verifiable facts;
- **Timely** – whilst it may be possible to delay some information, other information may be required immediately, and delays may be critical;
- **Secure** – partners must believe that any information they provide in confidence will be treated as such, and not used for commercial advantage or released for wider publication.

It may also be the case that partners wish to anonymise information that they wish to share in order to protect the information's source, or to avoid the possibility of commercial embarrassment. In order to achieve this, they may use a trusted intermediary to pass on the information, having first made certain that it contains nothing that might identify its originator. Such an individual may well be the Chair of the PPP, or a public sector representative who can have no commercial interest or bias.

In many instances, the sharing of information on a face-to-face basis is by far the most effective, but this is not always possible, especially in major incident situations, and therefore an electronic form of information sharing may be developed³¹⁸.

In 2011, ENISA produced the 'Cooperative Models for Effective Public-Private Partnerships: Good Practice Guide'³¹⁹. Whilst not prescriptive, this guide provides considerable detail on setting up and maintaining PPPs, including the answers to why? who? how? what? and when? Both public and private sector organizations looking to set up a PPP would benefit enormously from reading this document and taking advantage of the many suggestions and recommendations it contains.

Trust

The most important attribute of a PPP is that of trust. Members must be able to rely completely on the honesty and integrity of their fellow members, especially when dealing with sensitive commercial issues and areas in which national security is at stake. Indeed, it is normal for PPP members to be subjected to some form of security vetting in order to gain admission to the PPP. Trust can be divided into a number of distinct areas:

³¹⁸ David Sutton, **Trusted Information Sharing for Cyber Security Situational Awareness**, Elektrotechnik und Informationstechnik, (2015), Springer.

³¹⁹ See <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperative-models-for-effective-ppps>

- Trust that information shared with the membership is accurate and timely; that information which would benefit the PPP is not unreasonably withheld; and that information shared does not place any member at an operational disadvantage.
- Trust that information shared will be treated in confidence. It would be very simple for one organisation to gain competitive advantage over another by revealing detrimental information about it. The impact could be financial, regulatory, reputational or any combination of these. It is essential that such information stays within the trusted group and is not discussed elsewhere. A process for handling such information is discussed later.
- Trust that promised support will be delivered when required. When a major incident arises, organizations that are either unaffected by the incident or that have sufficient resources to survive it should agree in advance to support those organizations that are badly affected with manpower, equipment or whatever resources would improve the situation.

Trust takes time to develop, especially between organizations that would normally be in competition for customers and revenue. It may be difficult for some organizations to adapt to this way of thinking, but as long as the organisation's senior management are fully behind the concept, the remainder of the organisation will be obliged to follow suit.

Trust is easily broken. An indiscreet comment or a broken promise can wreck a trusted agreement, and will inevitably be difficult if not impossible to repair. It may be that the person who breaks the trust is expelled from the PPP, but even so, their replacement will have an uphill struggle to rebuild the broken trust.

The need for discretion, which engenders trust, is frequently cited in closed meetings in which the so-called 'Chatham House Rule'³²⁰ is invoked:

When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

This also allows people to express views as individuals, which may not be the same as those of the organizations they represent, and means that they need not be concerned that their organisation's reputation will be impaired through being publicly quoted.

Traffic Light Protocol

The correct handling of shared information is paramount, and therefore there must be a mechanism by which information can be classified according to its sensitivity, and which can be used comfortably by both government departments and commercial organizations without the need to cross-reference their information classification schemes.

³²⁰ See <http://www.chathamhouse.org/about-us/chathamhouserule>

This can be conveniently dealt with by the so-called ‘Traffic Light Protocol’³²¹, which classifies information as one of four colours:

- RED - Personal for named recipients only - In the context of a face-to-face meeting for example, distribution of RED information is limited to those present at the meeting, and in most circumstances will be passed verbally or in person.
- AMBER - Limited distribution - recipients may share AMBER information with others within their organisation, but only on a ‘need-to-know’ basis. The originator may be expected to specify the intended limits of that sharing.
- GREEN – Community-wide - information in this category can be circulated widely within a particular community or organisation. However, the information may not be published or posted on the Internet, nor released outside of the community.
- WHITE - Unlimited - subject to standard copyright rules, WHITE information may be distributed freely and without restriction.

This method of information classification is widely used in information sharing communities around the world since it is very simple to understand and implement.

Where the classification of information to be shared is concerned, trust works on two levels. Firstly, the originator must ensure that the information has been correctly classified, and must be confident that the recipients will handle the information in line with the classification. Secondly, recipients must have sufficient trust in the integrity of the originator so that they can have the same level of confidence in the reliability of the information.

Emergency exercises

In 2004, the PPP agreed that whilst plans were in place to respond to and recover from a major incident, it was important to verify by running exercises that these plans were fit for purpose. Ironically, the first meeting of the exercise working party took place on the same day that a major incident³²² occurred, reinforcing the requirement.

Prior to this, BT and Cable & Wireless had conducted joint exercises, but until 2004 there had never been involvement by the mobile networks, other fixed-line providers or the Internet community.

³²¹ See <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/information-disclosure>

³²² On 29th March 2004, a fire broke out in a cable tunnel beneath the city of Manchester, damaging a number of fibre optic and copper cables running between two major telephone exchanges, causing severe disruption to both public and private fixed-line and mobile services, mainly across the north of England. The resulting cooperation between members of the PPP reduced the downtime by several days, and most services were fully operational again in less than a week.

The first exercise took place in early 2005, and focussed on a number of unrelated but coincidental events supposedly located in two major cities. The post-exercise review identified a number of areas where arrangements could be improved, and by July 2005, when the mobile networks became severely overloaded during the London bombing incidents, the PPP members were significantly better prepared and responded quickly and effectively.

A further exercise took place in 2006, based on a severe weather incident, with the initial scenario being developed in conjunction with the Met Office. It was following the post exercise review for this that the team were invited to take an active role in the forthcoming government-run exercise for the electricity industry, 'Exercise Long Shadow'.

This brought about the first real contact between the emergency planning teams of the two CI sectors, and the exercise scenario was developed over a period of several months leading up to the event itself, at which the PPP's exercise team played a key role.

The planning alone for this exercise was a major milestone for the exercise team, since until then, the means by which a national power blackout would be recovered was completely unknown to them, and full participation in the exercise allowed both CI sectors to better understand how their respective networks worked and how they would be restored.

Following this, the planning team began the development of a similar exercise for the electronic communications sector – 'Exercise White Noise' – in which the failure of both the public fixed and mobile networks was simulated, but whilst allowing Airwave (the private mobile network) and the Internet to remain fully operational, since the underlying signalling/routing protocols are entirely different.

Further exercises have subsequently been run, testing different aspects of the electronic communications critical infrastructure, and all have contributed to the knowledge by both private and public sectors, allowing improved response to incidents and more efficient recovery.

Response to the London bombings in July 2005

On 7th July 2005, four separate bomb attacks took place in London. Three of these were on the underground system at Aldgate, Edgware Road and Kings Cross/Russell Square, and the fourth took place on a number 30 bus in Tavistock Square. 52 people died and 700 were treated for their injuries.

Within a short space of time following the first explosion, the mobile networks were suffering significant overload due to the number of mobile-originated calls being attempted by people caught up in the events and also mobile terminated calls from people trying to contact friends and family members known to be in London at the time.

In 2005, the Airwave network intended to provide secure private communications for and between emergency responders, was still in its early stages of rollout and public mobile cellular systems were heavily utilised by all emergency responders to enhance – and occasionally as a substitute for – the existing VHF and UHF private radio networks.

Several techniques were used initially by the mobile operators to increase the capacity in the affected areas, but the problem began to impact on the fixed-line network as well, and this was where the PPP was able to work together to resolve the problem by introducing ‘call gapping’, a technique that restricts calls entering the network at source rather than failing to connect further into the network. This implementation had an immediate and dramatic effect, reducing congestion and allowing both the fixed and mobile networks to remain fully in service, although later in the day at the request of the emergency services, part of the mobile network in the Aldgate area of the City of London was shut down for several hours.³²³

In the days immediately following the attacks, a number of organizations from the PPP worked with the emergency services and the London Resilience Team to establish a ‘family assistance centre’ providing support and communications facilities to both victims and families.

The control of response to major incidents

Whilst individual organizations have their own plans and procedures for responding to major incidents, the overall control and management is normally undertaken by the emergency services, usually headed by the Police. In England and Wales, this controlling organisation is referred to as Gold Command, which operates at a strategic level and is supported by Silver (the tactical level) and Bronze (the operational level).

When a major incident arises in which the electronic communications infrastructure is either adversely affected, or plays a major role in the response and recovery process, one or more representatives from the PPP will attend Gold Command meetings, providing up-to-date reports on network status and issues, and taking back requests for assistance or further information to the PPP via the conference calls.

Following the introduction of the Civil Contingencies Act 2004, regional resilience PPPs have been established in the UK, in which representatives from the electronic communications and other utilities meet regularly with regional government officials, increasing the knowledge of how their services are delivered, how they are recovered following major incidents, and how the regional resilience teams can work with them to improve resilience and respond more quickly when the need arises.

³²³ **Report of the 7 July Review Committee**, (2006), London Assembly, pp. 90-92, ISBN 1 85261 878 7

Figure 2 illustrates how the various organizations interact in the event of a major incident.

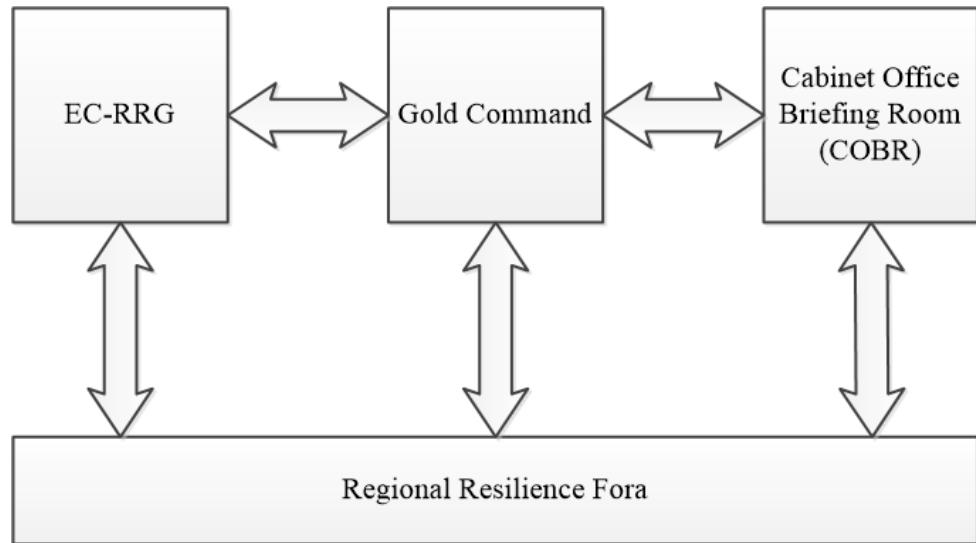


Figure 2 – Relationship between EC-RRG and other organisations

This shows the addition of the central government Cabinet Office Briefing Room (COBR), in which incidents having a major national or international impact are managed, chaired by the relevant lead government department.

Conclusions and recommendations

PPPs can be highly effective in responding to major incidents – indeed if the impact on such an incident is to be minimised, a PPP is an essential part of the higher level emergency response process. A well-engineered PPP will also play a significant role in the later stages of recovery from the incident and the return to normal or near normal status quo.

Firstly, there must be the will to bring about an organisation that can deliver tangible benefit to society, and should not be a ‘talking shop’, since this kind of organisation will rarely achieve anything useful in the long term. The initial concept may originate from a government department or a sector regulator – it is less likely to be at the instigation of a private sector organisation.

The initial meeting must present a solid series of objectives that allow the member organizations to understand what the PPP is designed to achieve, but will probably not be prescriptive about how this should happen. It is more beneficial to let the PPP develop its own ideas, but it must be recognised that this will take time.

It should be understood that there may well be fear and mistrust in the early stages. This is a natural state of affairs, considering that members of the PPP will initially think

of their organizations as rivals as opposed to partners. This will change, but again it will take time while mutual respect and trust are established and developed.

One way in which this can be improved is to engage the members in related group activities. In its early stages, members of the EC-RRG were given a tour of the National Grid Control Centres for both electricity and gas. Not only did this prove an interesting experience for the members, but it also allowed them to make contact with their peers in other sectors – something which was to prove advantageous later on, since contacts had already been established, and it is a well-known fact that the best business relationships begin with personal ones.

There should be a mechanism within the PPP for members to share information informally with a trusted individual, whether this is the Chair, or an unbiased public sector representative. This permits members to anonymise sensitive information and not to fear personal or organisational embarrassment. The person in whom this trust is placed is in some cases referred to as the ‘Trustmaster’, and must be able to demonstrate total integrity.

Members must decide for themselves what information can be shared and to what level, applying the appropriate level of classification using the traffic light protocol, and again this is a skill that will be developed over time.

Members should be encouraged to participate fully. Once the PPP is up and running, there will be many tasks that need to be undertaken. Some members will be more keen than others to take on work, but it is essential that everybody contributes as equally as possible, otherwise it will always be a core of people doing most of the work. Likewise, active participation in discussions and information sharing must be encouraged.

Whilst it may be advantageous to have the regulator or a government department chair the PPP in its early stages, in the longer term it will be more appropriate for the private sector to take over this role, and to rotate the position annually, the current deputy Chair taking over and a new deputy Chair being elected.

A Memorandum of Understanding should be drawn up. Since this must apply to both public and private organizations, this may well take many months to gain approval from all members, since their legal departments will take a close interest in the fine detail. This should not be the cause of delay in setting up the PPP, since it is more productive to begin to achieve the PPP's objectives than it is to reach a formal agreement on the terms and conditions. Amongst other things, the Terms of Reference will allow the PPP to define the qualifications for membership based on how the prospective member can contribute to the PPP's objectives.

Probably the most important document of all will be the Terms of Reference, which will define the PPP's purpose and objectives, and it is from this that the individual tasks will be derived. The ToR should be reviewed at intervals to ensure that it remains viable and practical.

In cases where a mechanism for alerting members of the PPP is required, this too should be developed at an early stage, since it may require several iterations with live

testing to prove its worth, and it should be expected that it is unlikely for the PPP to achieve a fully workable mechanism in a short space of time. This mechanism should be tested at irregular intervals, so that members do not anticipate the day of the test, and that failures to receive notification or to respond to the invitation should be followed up to ensure that they are not repeated.

Finally, members should set up a subset of the main PPP to develop and run exercises to test the plans and procedures, and to identify any gaps or overlaps in them. Exercise scenarios should be as realistic as possible, and can either replay incidents that have already occurred, or can create new imagined incidents. Exercises should always take members out of their comfort zone and stretch their organizations in responding to and recovering from the scenarios. As soon as possible following an exercise a review should be conducted, possibly by members who were not included in planning the exercise so as to make the review more objective. Output from these reviews may then be used as input for individual organisational improvement as well as for future exercises.

REFERENCES

Civil Contingencies Act 2004: <https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others>

Chatham House Rule: <http://www.chathamhouse.org/about-us/chathamhouserule>

Critical National Infrastructure: <http://www.cpni.gov.uk/about/cni/>

EC-RRG: <https://www.gov.uk/government/publications/role-of-the-telecommunications-industry-in-emergency-planning>

ENISA Good Practice Guide to PPPs:

<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperative-models-for-effective-ppps>

Exercise White Noise:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62283/bis-exercise-white-noise.pdf

Report of the 7 July Review Committee, (2006), London Assembly, pp. 90-92, ISBN 1 85261 878 7, and at

<http://www.london.gov.uk/sites/default/files/archives/assembly-reports-7july-vol3-individuals.pdf>

Thomas D. O'ROURKE, Arthur J. LEMBO, A and Linda K. NOZICK, **Lessons Learned from the World Trade Centre Disaster about Critical Utility Systems**, (2003), Cornell University, p. 277.* and at
http://www.colorado.edu/hazards/publications/sp/sp39/sept11book_ch10_orourke.pdf

Antii SILVAST and Joe KAPLINSKY, **White Paper on Security of European Electricity Distribution**, (2007), UNDERSTAND research project funded by the European Union, p. 35. And at http://understand.se/docs/White_Paper_EN.doc

David SUTTON, **Interdependency between Energy and Telecommunications**, (2009). ENISA Quarterly Review, ISSN 1830-3609. Volume 5, No. 3.

David SUTTON, **Trusted Information Sharing for Cyber Security Situational Awareness**, Elektrotechnik und Informationstechnik, (2015). Springer, ISSN 0932-383X.

EC-RRG Terms of Reference:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62280/ec-rrg-terms-of-reference.pdf

Traffic Light Protocol: <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/information-disclosure>

Rae ZIMMERMAN, **Public Infrastructure Service Flexibility for Response and Recovery in the September 11 Attacks at the World Trade Center**, (2003), Institute for Civil Infrastructure Systems, Wagner Graduate School of Public Service, New York University, p. 243.* and at
https://wagner.nyu.edu/files/faculty/publications/sept11book_ch9_zimmerman.pdf

Both these (*) papers are included in: **Beyond September 11th An Account of Post-Disaster Research**, (2003), Institute of Behavioral Science, Natural Hazards Research and Applications Information Centre, University of Colorado, at
<http://www.colorado.edu/hazards/publications/sp/sp39/BeyondSeptember11th.pdf>

(All links accessed on 10th September 2015.)

PUBLIC AND PRIVATE SECTOR ENERGY INFRASTRUCTURE AND CYBER INFORMATION SHARING

Ernest N. HAYDEN

ABSTRACT

Attention to critical infrastructure in the world continues to expand –especially following the events of Super Storm Sandy in the United States, the Philippine typhoon, and so forth. The energy infrastructure remains a domain receiving increased attention globally due to its importance to our society and national defense. Fortunately, due to increased awareness and attention by government agencies and energy company management, the security of these systems is improving. However, there continue to be substantial challenges in information sharing between the energy companies and the government and regulators and vice versa with the intention of increasing the security and resilience of this infrastructure. This discussion will summarize some of the actions taken to date –with emphasis on the United States experience– to encourage and facilitate improved information sharing and some of the barriers this process will be reviewed. Finally some possible solutions to this dilemma will be highlighted.

Key Words: Energy, Critical Infrastructure, Security, Information Sharing, US, ENISA

Introduction

Energy systems –especially electricity– are fundamental critical infrastructures in all countries of the world. Electricity is a daily imperative for the citizens, businesses, and governments and when interrupted, the end results range from simple inconvenience to critical failure of basic government and business operations. With the reliance on the Internet and the communications systems required to support the transfer of the data and bits and bytes loss of electric service can be a very serious impediment. Even efforts focused on disaster recovery and assessment are relying more and more on the Internet, cellular telephone networks, and global information systems (GIS). Hence, without electricity, chaos can be the result at the social level.

In many countries, the electric grid and supporting systems are owned and operated by government or semi-government agencies. However, in the United States (US)

most electric grid infrastructure is owned and operated by private companies. Regardless of ownership, it is critical that these large systems and expensive components such as transformers be secured from both physical and cyber attacks. However, defense of these systems is best done by sharing information on vulnerabilities, ways and means of defense, and intelligence on those who wish to do harm to the electric grid for malicious intent or simple vandalism. This chapter focuses on information sharing for electric grid defense and will primarily rely on examples and cases from the United States.

Model of Information Sharing

You don't exchange business cards in the middle of a crisis. You have to build the social network before.

Eric Luijif and Allard Kernkamp³²⁴

A simple way to look at the information sharing approach is a triangle of government, private business and private citizens. Essentially optimal information sharing is an open flow of ideas and concerns from the government to the businesses and citizens and equivalent flows of information from the businesses/private citizens back to the government. And, of course, the flow of information between the citizens and the businesses is also desired. Unfortunately, the open and unimpeded flow of information between and among these different institutions and individuals can be slowed –or even blocked– due to a variety of challenges such as politics, intellectual property protection, legal concerns and ultimately a lack of trust.

But, what is driving this need for increased exchange of vulnerabilities, threats, advisories and warnings? The electric grid is under attack.

Drivers for Information Sharing – Why Do This?

In a recent article in *Forbes* business magazine, Ken Silverstein observed, “America’s energy infrastructure is getting bombarded through cyber warfare –attacks that are getting through and which if the big one hits, would signal lights out on huge population centers. It’s not a computer game. It’s real, which is constantly testing corporate resolve.”³²⁵ We are also seeing physical attacks on energy infrastructure such as the

³²⁴ Ayhan Güçüyener, “Criticality of Information Sharing for Cyber Security and Models for Energy Sector”, Hazar Strategy Institute (HASEN), 2015.

<http://www.hazar.org/blogdetail/blog/criticality-of-information-sharing-for-cyber-security-and-models-for-energy-sector-1262.aspx>.

³²⁵ Ken Silverstein, “Utilities Engaged In Hand-To-Hand Cyber Combat To Keep The Lights On - Forbes” *Forbes*, 2015, <http://www.forbes.com/sites/kensilverstein/2015/09/13/utilities-engaged-in-hand-to-hand-cyber-combat-to-keep-the-lights-on/>

Metcalf substation transformer shooting³²⁶ in California, USA, and explosion on the Turkish pipeline in 2014.³²⁷

There is substantial conversation and debate about the best strategies to follow to protect the energy infrastructure from these attacks, one point of general agreement among cyber analysts is the need for enhanced and timely exchange of cyber and physical threat intelligence both within the private sector and between the private sector and government.³²⁸ In the US there are several voluntary structures and processes for information sharing. Also, the North American Electric Reliability Corporation (NERC)³²⁹ has imposed a rule on the major electric transmission companies to report any cyber attacks or incidents on critical electric grid controls and systems to the Electricity Information Sharing and Analysis Center (E-ISAC)³³⁰ and failure to do so could result in a financial penalty to the company.

Globally, however, it does make sense that information on physical and cyber vulnerabilities, threats and case studies of recent attacks and near-misses be communicated to all affected parties. This includes domestic information sharing as well as international exchange –especially because the Internet truly does not observe any international boundaries. Cyber attacks on the electric grid can come from another country or another continent. Also, electricity crosses international boundaries in many instances, so a cyber attack in one adjacent country can affect the power grid in its neighbor.

Knowledge of these threats is critical to enabling an effective defense. Thus, exchange of information in a timely manner is an intelligent action; however, the burden on data exchange prevent ready information transfer and may result in the unintended consequences of a successful attack that could have been prevented if the defender had been warned early enough.

Benefits of Information Sharing in Mitigating Cyber and Physical Threats

There are several benefits of information sharing in mitigating cyber threats. First, if one organization is being attacked via cyber means, then by telling others of this event will help the other entities better protect themselves from the attack, or, at a minimum,

³²⁶ Alexis C. Madrigal, "Snipers Coordinated an Attack on the Power Grid, but Why?" *The Atlantic*, 2014, <http://www.theatlantic.com/technology/archive/2014/02/snipers-coordinated-an-attack-on-the-power-grid-but-why/283620/>

³²⁷ Jordan Robertson, Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyber War." *Bloomberg Business*, 2014, <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>

³²⁸ Andrew Nolan, "Cyber Security and Information Sharing: Legal Challenges and Solutions, Congressional Research Service", Washington DC, 2015.

<http://www.fas.org/sgp/crs/intel/R43941.pdf>

³²⁹ NERC Staff. "Electricity ISAC" NERC Webpage, 2015, <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>

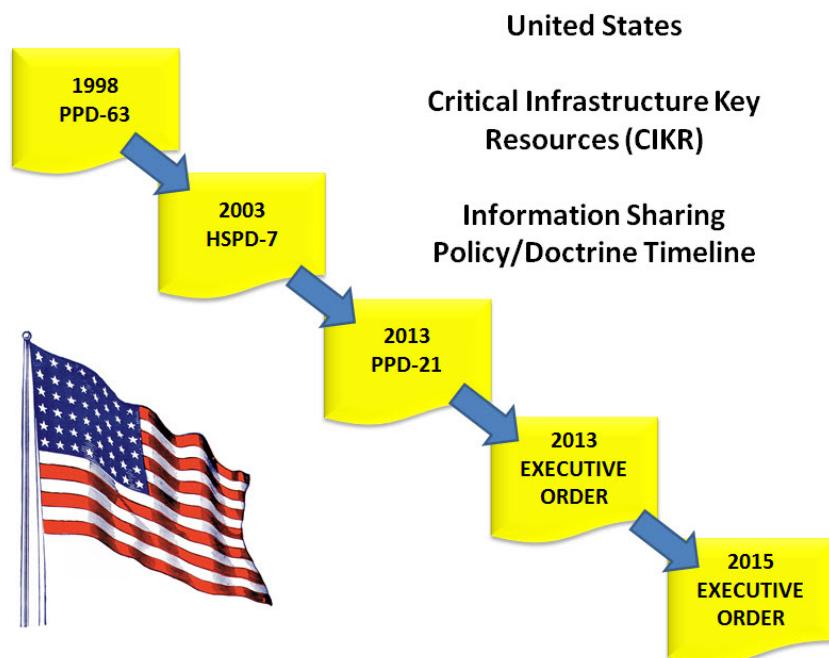
³³⁰ NERC Staff. "E-ISAC | Electricity Sector Information Sharing & Analysis Center," E-ISAC Webpage, 2015, <https://www.esisac.com/>

help the other entities look for symptoms that they have been attacked by the same invader. Secondly, by sharing this information –especially to an organization like the E-ISAC– then the attacks can be trended and better monitored in a more holistic, broader scope manner. Thirdly, by sharing information on attacks in progress or ways to better mitigate cyber threats, such as lessons learned, the trust level between the different organizations increases, allowing for faster and more effective communications when a cyber event is detected or new cyber protection measures are developed.

US Perspective and History

Since 1998 the United States government has been emphasizing the concept of critical infrastructure and its protection. As part of this protection concept, the idea of information sharing between the government, private sector, and within the private sector has been a point of discussion. A brief history of the information sharing directives from the US government is offered followed by a discussion on how the information sharing processes are organized.

Figure 1. US CIKR Information Sharing Timeline



History

The US government has been an active driver in the pursuit of information sharing among and between critical infrastructure sectors since 1998 with the publication of Presidential Decision Document 63 (PDD-63) issued under the Clinton administration.³³¹ PDD-63 identified electric power as a critical sector along with 14 others such as telecommunications, banking and finance, transportation, water systems and emergency services.

PDD-63 established the concept of an Information Sharing and Analysis Center (ISAC)³³² with the intent to "...strongly encourage the creation of a private sector information sharing center". PDD-63 continued to note that such a center could serve as a mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the government. Also, the ISAC could play a role gathering, analyzing and disseminating information from the government to the private sector.

In December 2003, then President George W. Bush issued Homeland Security Presidential Directive/HSPD-7 entitled "Critical Infrastructure Identification, Prioritization, and Protection."³³³ This directive was issued under the auspices of the attacks of 9/11 on the World Trade Center in New York City and the Pentagon in the US national capital. HSPD-7 did supersede PDD-63. Paragraph 25 of the HSPD continued to emphasize "...collaboration with appropriate private sector agencies and continue to encourage the development of information sharing and analysis mechanisms." In several places, the HSPD-7 emphasizes the need for the US Government to work with the State and local governments and the private sector in accomplishing the objectives of the directive.

A view of the Bush Administration's perspective of information sharing to protect critical infrastructure is in the Figure below from the National Strategy on Information Sharing (NSIS).³³⁴

³³¹ Clinton Administration Staff, "Critical Infrastructure Protection (PDD-63)", Washington DC: US Executive Branch, 1998. <http://fas.org/irp/offdocs/pdd/pdd-63.htm>

³³² Pronounced "eye-sack".

³³³ Bush Administration Staff, "Homeland Security Presidential Directive/HSPD-7." Washington, DC, 2003. http://www.isaccouncil.org/images/HSPD_7.pdf

³³⁴ Bush Administration Staff, "NSIS - Introduction and Overview." *National Strategy for Information Sharing*, 2007. <http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionI.html>

Figure 2. National Strategy on Information Sharing – 2007 (Bush Administration)



Foundations of the National Strategy for Information Sharing

In February 2013, President Barack Obama issued Presidential Policy Directive 21 (PPD-21).³³⁵ This directive, “Critical Infrastructure Security and Resilience,” was issued with the intention to strengthen and maintain secure, functioning and resilient critical infrastructure. This directive identified three strategic imperatives which included:

1. Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience,
2. Enable efficient information exchange by identifying baseline data and systems requirements for the Federal Government, and
3. Implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure.

³³⁵Obama Administration Staff, “Presidential Policy Directive -- Critical Infrastructure Security and Resilience PPD-21”, White House Webpage, 2013. <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

This directive also identified 16 critical infrastructures which slightly modified the sectors identified in PPD-63 and HSPD-7. These sectors include:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

As practiced in previous presidential directives, this directive revokes Homeland Security Presidential Directive/HSPD-7, issued on December 17, 2003.

On the same day PPD-21 was promulgated, President Obama also issued an Executive Order titled “Improving Critical Infrastructure Cyber Security”.³³⁶ In conjunction with his emphasis in PPD-21 on information sharing for improved security and resilience, his Executive Order also explicitly stated in Section 4, “It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with US private sector entities so that these entities may better protect and defend themselves against cyber threats.”

On February 13, 2015 –a year plus one day after the President’s Executive Order directing NIST to build the new Cybersecurity Framework– President Obama issued an Executive Order entitled “Promoting Private Sector Cybersecurity Information Sharing”.³³⁷ Again, as with PPD-21, the policy emphasis by the Obama administration was to improve and enhance the movement of information –especially cyber security threat information– as close to real time as possible. This Executive Order was issued to “...encourage the voluntary formation of (information sharing) organizations, to

³³⁶ Obama Administration Staff, “Executive Order -- Improving Critical Infrastructure Cyber Security.” White House Webpage, 2013. <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

³³⁷ Obama Administration Staff, “Executive Order -- Promoting Private Sector Cyber Security Information Sharing.” White House Webpage, 2015. <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>

establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.” Interestingly enough, this Executive Order “strongly encourages” the development and formation of Information Sharing and Analysis Organizations (ISAOs) and does not address the currently established formation of the ISACs.³³⁸

More about the ISAC Concept

At the US National Council of ISACs website^{339,340} there is a concise description of ISACs as follows:

“ISACs are trusted entities established by Critical Infrastructure Key Resource (CIKR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with the government. ISACs take an all-hazards approach and have strong reach within their respective sectors, with many reaching over 90 percent penetration. Services provided by ISACs include risk mitigation, incident response, alert and information sharing. The goal is to provide users with accurate, actionable, and relevant information. Member benefits vary across the ISACs and can include: access to a 24/7 security operations center, briefings, white papers, threat calls, webinars, and anonymous CIKR Owner/Operator reporting.”

³³⁸ As of this writing the subject of ISAOs versus ISACs and which organization type and approach takes precedence is still under active review and discussion. For one perspective on the formation of the ISAOs versus the ISACs, please see the *Infrastructure Security Today Blog* “Executive Order Promoting Private Sector Info Sharing,” at <http://infrastructuresecuritytoday.blogspot.com/2015/02/executive-order-promoting-private.html>

³³⁹ <http://www.isaccouncil.org/>

³⁴⁰ The US Council of ISACs website contains an excellent historical collection of key documents on the ISACs, ISAC formation, information sharing and organization from 2003 until 2010. The publications page can be found at: <http://www.isaccouncil.org/publications.html>

In 2004 ISACs were formed for the following CIKR sectors:

Table 1. ISAC Population as of 2004 (Reference: ISAC Council White Paper January 31, 2004)³⁴¹

ISAC
ISAC Council
Chemical ISAC
Electricity Sector ISAC (ES-ISAC)
Energy ISAC (Primarily Oil and Gas)
Financial Services ISAC (FS-ISAC)
Health Care ISAC
Information Technology ISAC (IT-ISAC)
Surface Transportation ISAC (ST-ISAC)
Public Transit ISAC (PT-ISAC)
Telecommunications Infrastructure ISAC (Telecom ISAC)
Truck ISAC
Water ISAC

It should be observed that the ISAC population has ebbed and flowed since 2004 but for the electric energy sector, the ES-ISAC –now called the E-ISAC– continues to be strong and a very active player in information security for the electric energy sector in the US and even parts of Canada.

The Electric Sector ISAC (ES-ISAC or E-ISAC)

Since 1998, the ES-ISAC has been providing security services to electricity service owners and operators in the US, Canada and parts of Mexico. The ISAC is operated on behalf of the Electricity Subsector CIKR by the North American Electric Reliability Corporation (NERC).

The mission of the ISAC is to be the trusted source for Electricity Subsector security information. The ISAC gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the Electricity Subsector, across interdependent sectors, and with government partners. The ISAC, in collaboration with the US Department of Energy³⁴² and the Electricity Subsector Coordinating Council (ESCC),³⁴³ serves as the primary security

³⁴¹ ISAC Council. *Reach of the Major ISACs*, 2004,
http://www.isaccouncil.org/images/Reach_of_the_Major_ISACs_013104.pdf

³⁴² <http://www.energy.gov>

³⁴³ The role of the Electricity Sub-sector Coordinating Council (ESCC) is to foster and facilitate the coordination of sector-wide policy-related activities and initiatives to improve the

communications channel for the Electricity Subsector and enhances the subsector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The ES-ISAC facilitates the flow of electricity-specific information among a wide range of Electricity Sector stakeholders. The ES-ISAC receives security information from member Electricity Subsector entities, public-private partnerships, government, and third parties. Through ISAC operations, analysis, and controls, the ES-ISAC transforms information it receives into value-added products and services shared with its members and stakeholders.³⁴⁴

All vetted electricity owners and operators in North America may participate in the electricity sector ISAC activities. Although the framework is a US government construct, the ISAC extends across the bulk power system territory which includes all of the US and Canada and portions of Mexico. Suggested members should include titles of Chief Security Officer, Security Director, Security Supervisor, and Intelligence/Information Analysts. Membership is free.³⁴⁵ However, vendors and contractors cannot become members of the ES-ISAC/E-ISAC.

As captured in the ESCC Strategic Review of the Electricity Sector Information Sharing and Analysis Center dated July 9, 2015 and noted in the ES-ISAC website, key ES-ISAC products and services to the electricity sector and government include the following:

reliability and resilience of the Electricity Sub-sector, including physical and cyber security infrastructure. The ESCC consists of one member from the NERC Board of Trustees (appointed by the board chairperson), the NERC Chief Executive Officer (CEO), five CEO-level executives from NERC member organizations, and the chairperson of the NERC Critical Infrastructure Protection Committee. The key roles of the ESCC are to represent the Electricity Sub-sector, to build relationships with government and other critical infrastructure sectors, and to participate in joint initiatives as part of the "partnership framework" envisioned by the National Infrastructure Protection Plan and Energy Sector-Specific Plan. Some of these initiatives are information requests, while others require regular participation on formally established working groups. The Electricity Sub-sector receives many requests from government departments and agencies and other critical infrastructure sectors to participate in various initiatives. The ESCC keeps informed of these efforts, and participates directly when necessary. For more information please see:

<http://www.nerc.com/pa/CI/Pages/ESCC.aspx>

³⁴⁴ Gerry Cauley, Reasor, Jackson and William H Spence, *Roles of the Electricity Subsector's ISAC and Coordinating Council*, Atlanta, GA. 2015, p. 2.

[http://www.nerc.com/gov/bot/botquarterlyitems/Policy Input Package August 2015 PUBLI C POSTING.pdf](http://www.nerc.com/gov/bot/botquarterlyitems/Policy%20Input%20Package%20August%202015%20PUBLI%20C%20POSTING.pdf)

³⁴⁵ NERC Staff, Op cit.

Key Information Sharing Forums:

ES-ISAC Briefing Series – Participation in the monthly webinar series has grown to more than 250 members each month. The series is a useful and relevant source of information for security and nonsecurity professionals.

ES-ISAC Portal – Registered portal users have grown to more than 2,800 individuals from nearly 800 organizations. This self-service platform provides members with access to blogs, watch lists, alerts, and other security information and analysis products. (A new, more capable platform has been launched under the moniker “E-ISAC” in October 2015).

Key Analysis and Validation:

ES-ISAC Weekly Security Blog – Summarizes cyber and physical security reports from the past week and identifies relevant news reports and upcoming events.

ES-ISAC Watchlist Entries – Specific and actionable indicators of compromise related to incidents and other activities observed in the Electricity Subsector, other sectors, and the government that are targeted at IT and security personnel. Release cycle to members is hours to days.

NERC Alerts – Vulnerability or threat information pertaining to high or potential high impact events on the bulk power system (BPS) as defined by NERC Rules and Procedure. Release cycle to members is days or weeks.

Cyber Security Risk Information Sharing Program (CRISP) – The program uses Information Sharing Devices to collect and transmit security information from electricity operator participant sites. Pacific Northwest National Laboratory analyzes and integrates this information with classified government sources and collaborates with the ES-ISAC to identify threat patterns and trends across the Electricity Subsector. Data is shared with CRISP participants, and then unattributed data is shared with the broader ES-ISAC membership.

Hydra – As security issues arise with potentially significant sector impact, actions taken by the ES-ISAC may include forming up a team of asset owners and other trusted experts to focus on the challenge, drive for clarity including appropriate mitigations, and share insights gained with the sector through the ES-ISAC with product releases, such as Bulletins and Alerts.

Key Industry Exercises and Events:

Grid Security Exercise (GridEx) Series – This biennial geographically distributed (U.S., Canada, and Mexico) exercise is used to better understand industry response to a major event and take away valuable lessons learned. GridEx is the only electricity-centric exercise that includes industry, government, and cross-sector security issues

and participation. More than 2,000 participants from 234 organizations attended GridEx II.

Grid Security Conference (GridSecCon) – The annual conference allows industry, government, academia, and the ES-ISAC to engage in timely and open conversation about threats, vulnerabilities, and reliability risk to the BPS.

Cyber Security Risk Preparedness Assessment (CRPA) – More than 60 participants attended one of two workshops conducted this year that focused on developing and facilitating a custom, operationally informed, incident response tabletop exercise, followed by analyzing and reporting results. In addition, the ES-ISAC is working with trained third party providers to help encourage the use of CRPAs and share results to help inform overall industry level results, while also aiming to reduce directly-funded ES-ISAC resourcing associated with individual engagements.

So, why did the ES-ISAC change its name to E-ISAC? “Our ISAC was the only one that used the term ‘sector’ in its title. We made a small change to our name to bring us in line with other critical infrastructure ISACs,” said Marcus Sachs, senior vice president and chief security officer. “Our portal is the virtual face of the E-ISAC. This new look and feel is one of many steps we are taking to improve the way we interact with asset owners and operators in the electricity sector.”³⁴⁶

One last perspective regarding the E-ISAC is the scope of its information sharing. Specifically, the E-ISAC is the lead information sharing and analysis nexus for the entire electric sector –not just bulk power (i.e., electric transmission). By the way, the E-ISAC does not monitor the “physics” of the grid such as voltage, frequency, etc. That is performed by another group within NERC called the Bulk Power Awareness Team.

More about CRISP – Cyber Security Risk Information Sharing Program

CRISP is a public-private partnership formed in 2014 to facilitate timely sharing of cyber threat information and develop situational awareness tools to enhance the Electricity Sector’s ability to identify, prioritize, and coordinate the protection of its associated critical infrastructure.³⁴⁷ CRISP has established a partnership between the Department of Energy’s Office of Electricity Delivery and Energy Reliability (DOE/OE), the E-ISAC, Pacific Northwest National Labs (PNNL), Argonne National Lab (ANL), and participating companies. CRISP does not replace other US Government efforts to provide cyber security assistance or information sharing.

CRISP was designed to develop and maintain an effective system for collaboration among energy sector stakeholders, trade groups, NERC, the US Department of

³⁴⁶ Mielcarek, Kimberly. “Electricity ISAC Renamed, New Portal Launched With Improved Look and Performance.” *NERC Webpage*, Atlanta, GA. 2015.

http://www.nerc.com/news/Headlines_DL/ISAC_Web_24SEP15.pdf

³⁴⁷ US Department of Energy, “CRISP-Cyber Security Risk Information Sharing Program”, Washington DC, 2015, p.1.

Homeland Security (DHS), the US Federal Bureau of Investigation (FBI) and the US intelligence community by providing bi-directional information sharing of actionable information related to the detection, prevention, mitigation and rapid response to potential threats.³⁴⁸

The CRISP system requires that participating entities install an Information Sharing Device (ISD) on their network border just outside the corporate firewall. The ISD collects data and sends this data in encrypted form to the CRISP Analysis Center at PNNL. The CRISP Analysis Center analyzes the data and, using government furnished information, sends alerts and mitigation suggestions back to the participating entities about potential malicious activity. CRISP also generates other situational analysis information such as hostile IP addresses, DNS domains, etc.³⁴⁹

Fusion Centers and their Role in Information Sharing

In 2007, Appendix I of the National Strategy for Information Sharing³⁵⁰ established a national integrated network of state and major urban area Fusion Centers to aid and facilitate in information sharing to protect critical infrastructure. The Fusion Centers serve as primary focal points in the US state and local –normally urban– environment for the receipt, gathering and sharing of threat-related information. The Fusion Centers are not dedicated to a specific CIKR sector but instead provide information and support to front-line law enforcement, public safety, fire services, emergency response, public health, and private sector security personnel. The Fusion Centers also provide interdisciplinary expertise and situational awareness. The focus of the Fusion Centers is primarily to counter crime and terrorism. Fusion Centers are owned and operated by state and local entities with support from federal partners.³⁵¹

Again, the Fusion Centers are not specific to the Electricity Subsector nor are they exclusively cyber security oriented, but they can contribute to the protection of the electric/energy grid with the dissemination of threat information.

ENISA and European Information Sharing

ENISA is the European Network and Information Security Agency with offices in Athens, Greece. The Agency's mission is essential to achieve a high and effective level of Network and Information Security within the European Union (EU). Together with

³⁴⁸ Security Dispatch, “DOE Enhances Cyber Security Risk Information Sharing Program - Darkmatters.” *DarkMatters*, 2015, <http://darkmatters.norsecorp.com/2014/11/07/doe-enhances-cybersecurity-risk-information-sharing-program/>

³⁴⁹ Of note, there has been some criticism of the CRISP program relative to the players, their conflict of interest in the project and results, and the lack of maturity of the sensor technology. For more comments please see

<http://www.digitalbond.com/blog/2014/11/13/crisp-market-failure-and-fools-gold/>

³⁵⁰ Bush Administration Staff, “National Strategy for Information Sharing” 2007, <http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionIX.html>

³⁵¹ US Department of Homeland Security, “National Network of Fusion Centers Fact Sheet,” 2015, <http://www.dhs.gov/national-network-fusion-centers-fact-sheet>

the EU-institutions and member states, ENISA seeks to develop a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organizations in the European Union. ENISA is helping the European Commission, the member states and the business community to address, respond and especially to prevent network and information security problems.³⁵²

ENISA has three primary approaches to information sharing. First, it supported the European Financial Institutes –Information Sharing and Analysis Centre (FI-ISAC) founded in 2008.³⁵³ Secondly, it views its role as a community trust builder.³⁵⁴ Thirdly, it facilitates information sharing between the various member states and the various Computer Emergency Response Teams (CERTs).³⁵⁵

In 2010, ENISA worked on an analysis of barriers to and incentives for information sharing in the field of Critical Information Infrastructure Protection (CIIP). The report looked at such issues as economic incentives for information sharing and the current barriers to satisfactory intelligence exchange. The report did identify the most important barriers and offered recommendations for both public decision makers and private sector stakeholders.

Please note that this study was for the broader view of CIIP and not specific to the electricity sector.

The study resulted in a report entitled *Incentives and Barriers to Information Sharing in the Context of Network and Information Security*.³⁵⁶ This report did identify barriers but it also identified 20 recommendations across the European Institutions/ENISA, National Governments, and Private Sector.

Overall, ENISA has facilitated several studies on selected cyber information issues resulting in “Good Practice Guides”. A selection of the key ones relative to this topic includes:

- **Alerts, Warnings and Announcements – Best Practices Guide (2013)**

This guide complements the existing set of ENISA guides that support Computer Emergency Response Teams (CERTs, also known as CSIRTs). It describes good practices and provides practical information and guidelines

³⁵² <https://www.enisa.europa.eu/about-enisa>

³⁵³ European Union Agency for Network and Information Security, “Information Sharing”, *ENISA Web Page*, 2015, <https://www.enisa.europa.eu/activities/cert/support/information-sharing>

³⁵⁴ Ibid.

³⁵⁵ Ibid.

³⁵⁶ European Union Agency for Network and Information Security, “Incentives and Barriers to Information Sharing”, 2010, <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing>

for the process of preparing and issuing alerts, warnings and announcements to a CERT's constituency.³⁵⁷

- **Cooperative Models for Effective Public-Private Partnerships – Good Practice Guide (2011)** This guide builds on the desktop research, which revealed a set of characteristics that can be used to describe these public-private partnerships (PPPs) in a common form despite their diversity. The results from 30 questionnaires and 15 interviews consolidated and validated a taxonomy, presented in the desktop research as a supporting document, and revealed five main components addressing the *Why, Who, How, What* and *When* questions associated with creating and maintaining PPPs. This data was collected from both public and private sector stakeholders across 20 countries.³⁵⁸
- **Good Practices Guide on Reporting Security Incidents (2009)** This document examines these practices by first giving a more detailed introduction to the subject of incident reporting and then reviewing the lifecycle of an incident reporting and information sharing scheme.³⁵⁹
- **Good Practice Guide – Network Security Information Exchanges (NSIEs) (2009)** The main aim of this guide is to assist member states and other relevant stakeholders in setting up and running NSIEs in their own countries.³⁶⁰

The last guide on NSIE's is a seminal “textbook” on setting up cyber security information sharing methodology. The 49-page guide offers practical guidance on such issues as:

- Overview of NSIEs
- Observed Characteristics of an NSIE
- Building Trust in an NSIE
- Interfaces with an NSIE (e.g., law enforcement, CERTs, etc.)
- Funding and Costs

³⁵⁷ European Union Agency for Network and Information Security, “Alerts-Warnings-Announcements”, 2013, <https://www.enisa.europa.eu/activities/cert/support/awa>

³⁵⁸ European Union Agency for Network and Information Security, “Good Practice Guide on Cooperative Models for Effective Public Private Partnerships”, 2011, <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperative-models-for-effective-ppps>

³⁵⁹ European Union Agency for Network and Information Security, “Good Practice Guide on Incident Reporting”, 2009, <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1>

³⁶⁰ European Union Agency for Network and Information Security, “Good Practice Guide on Information Sharing”, 2009, <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide>

- Legal Considerations
- Actions to Set Up and NSIE
- Useful Appendices (e.g., Traffic Light Protocol (TLP), Chatham House Rule, etc.)

Barriers and Obstacles for Information Sharing

Admittedly if information sharing were simple and easy to do, the US, ENISA, and other leading governments would have robust and highly effective information sharing capabilities in place. However, that is not as simple to enact as one would suspect due to a variety of challenges ranging from legal issues to privacy concerns, to lack of perceived value and –the biggest barrier of all– lack of mutual trust. This section reviews these barriers and obstacles for information sharing.

In summary, the key barriers and obstacles can be listed as follows:

- **Legal:** Privacy Laws, Antitrust Laws, Tort Law
- **Concerns:** Intellectual Property, Regulatory Enforcement, Freedom of Information Act (US)
- **Barriers:** Financial Barriers, Public Reputation, Lack of Perceived Value to Exchange Information, Lack of Mutual Trust

The Concept of Information Sharing

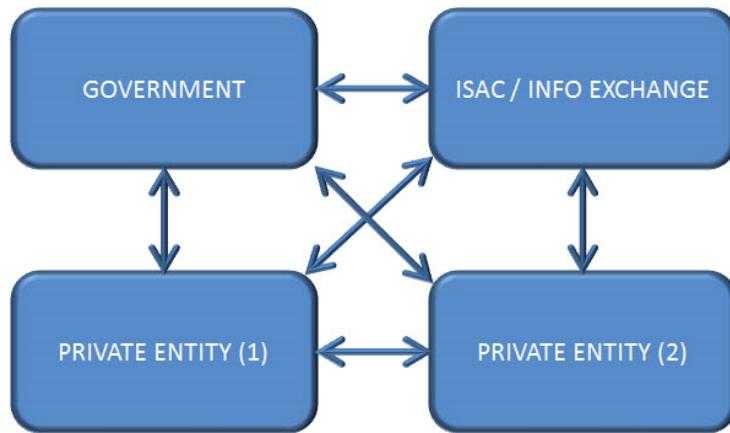
While often the concept of “cyber information sharing” is thought of as a monolith, the sharing of cyber intelligence touches on three related but distinct concepts.³⁶¹ First, cyber information sharing is used in the context of dissemination of cyber intelligence from the Federal Government to other government entities or the private sector.

Second, cyber threat intelligence dissemination includes private sector entities sharing cyber intelligence with each other.

Finally, cyber information sharing also includes when private entities share cyber threat information in their possession with the government.

³⁶¹ Andrew Nolan, “Cyber Security and Information Sharing: Legal Challenges and Solutions”, *Congressional Research Service*, Washington DC, 2015, <http://www.fas.org/sgp/crs/intel/R43941.pdf>, p.5.

Figure 8. Elementary View of Information Sharing



Legal Issues with Information Sharing – Government to Private Sector³⁶²

From a high-level view –specifically with a US-centric perspective– there are several legal issues that immediately surface relative to the movement and exchange of information from the Government to the private sector. Some US laws may limit the ability of the government to disseminate cyber threat information to private entities. The Homeland Security Act itself requires the US Department of Homeland Security (DHS) to ensure that any intelligence in its possession "...is protected from unauthorized disclosure and handled and used only for the performance of official duties." More specifically the Act mandates that DHS adhere to a) the requirements of the National Security Act of 1947 and b) any authorities of the Attorney General "concerning sensitive law enforcement information".³⁶³ Because of these legal restrictions and constraints, sharing information that is viewed as sensitive, classified or part of a cyber crime investigation may be very limiting. Also, if the private entity does not possess an adequate or up-to-date security clearance, then DHS (or other Federal Government Agency) may not release the information due to concerns over "protection from unauthorized disclosure".

Hence, the “free flow” of cyber information from the government to the private sector is prevented due to legal constructs alone.

³⁶² An excellent summary of legal issues preventing ready exchange of cyber information in the US is the Congressional Research Service (CRS) report, “Cyber Security and Information Sharing: Legal Challenges and Solutions”, written by Andrew Nolan, <http://www.fas.org/sgp/crs/intel/R43941.pdf>

³⁶³ Andrew Nolan, “Cyber Security and Information Sharing: Legal Challenges and Solutions”, *Congressional Research Service*. Washington DC, 2015, <http://www.fas.org/sgp/crs/intel/R43941.pdf>, p. 11.

Legal Issues with Information Sharing – Private Sector

In the US the laws governing the dissemination of cyber threat information to the private sector is relatively straightforward; however, the legal backdrop regarding sharing cyber intelligence in the possession of private parties is much more complicated. Unfortunately, there are several legal concerns that “create disincentives”³⁶⁴ against sharing such information.

Antitrust/Anti-competition

An often-cited legal concern that slows down or stops cyber information exchange is about anti-competitive issues such as violation of US Federal Antitrust Law. In spite of some legal interpretations over the legality of sharing information between private entities (such as companies) relative to antitrust laws, there is no case law that addresses how antitrust laws apply to coordinated efforts to combat cyber threats. The net result is considerable legal uncertainty for private entities that may want to exchange relevant information; however, the easiest approach is to not submit the data.³⁶⁵

It would not be out of the question if other country governments have similar concerns with the control of government intelligence on the threats to the electric grid infrastructure and as such hold the info back from the companies that need it.

Tort Law

Another private sector concern that discourages the dissemination of security and threat intelligence is tort law, specifically those based upon negligence. Here, the private entity may be concerned that sharing and obtaining cyber information may result in a liability and legal action focused on “failure to act” upon threat information. Hence, after a cyber attack, an injured party may sue an electric utility for failure to protect its network if they knew that such an attack was viable and possible.

For example, imagine an electric utility sharing cyber attack information with an ISAC. One perception is that the company may be admitting that it could have foreseen the attack or mitigated its effects in some manner thus providing potential plaintiffs with credible evidence to support a potential tort lawsuit. The same approach could apply to those who receive information about a potential cyber attack, fail to act and defend the threat, and can no longer claim the harm from the cyber attack was unanticipated.³⁶⁶

Again, the theme of this issue is that it may be easier for an entity to not share information in order to avoid legal action due to a perceived “lack of action”.

³⁶⁴ Ibid, Page 12.

³⁶⁵ Ibid, Page 28.

³⁶⁶ Ibid, p. 30.

Intellectual Property Concerns

Another concern and subsequent barrier to information sharing from the private sector to the government or an ISAC is related to intellectual property protection, or loss thereof. The issue is that should information be shared with the government this could be interpreted as the entity waiving all intellectual property rights associated with such information.³⁶⁷ In a similar manner, a private entity may worry about the loss of trade secret protection for any information shared that is associated with cyber threat intelligence.

This concern can be minimized through some means such as negotiations to protect the information before the transfer of the knowledge. However, in the US in order to gain information to some government cyber intelligence information, a private entity must sign a Cooperative Research and Development Agreement (CRADA) with the government agency in question. The text of the CRADA reportedly includes language that potentially forfeits intellectual property rights on the shared material and information.³⁶⁸

Again, losing intellectual property and trade secret protection is a substantial barrier to open and unencumbered information exchange between the private sector and the government.

Regulatory Enforcement Concerns

Considering that the issue with shared information being given to the government that results in a regulatory investigation or even a fine or jail time for the executives, there can be a fear that the government still use this shared cyber security information against the private entity if the underlying information pertains to a cyber breach resulting in a loss of personal or regulated data.³⁶⁹

A recent example of such a concern occurred in the United States in 2014 where a hotel chain had a data breach, made notification as required by the effective data breach laws and then subsequent investigation by the US Federal Trade Commission (FTC) led to enforcement actions resulting in millions of dollars in civil penalties, more than 50 private settlements, and expensive compliance obligations for the company under investigation.³⁷⁰

US Freedom of Information Act Disclosures

The US has a law called the Freedom of Information Act (FOIA) that allows citizens to petition the US Federal Government to release information in their possession that

³⁶⁷ Ibid, p. 36.

³⁶⁸ Ibid, p. 37.

³⁶⁹ Ibid, p. 37.

³⁷⁰ Ibid, p. 38.

may be declared classified but, for the good of society, should be released for public review. A useful website is at <http://www.foia.gov/>.

The scenario of concern by a private entity is that the organization provides cyber security intelligence to the Federal Government with the intention of sharing information to protect others. The Federal Government may consider this information classified and protect it accordingly. However, a FOIA request is submitted and after a review and perhaps judgement the information released by the private entity under confidence to the Federal Government is released for others to view. This scenario is often considered by the private entities before they submit information to the government and in some cases blocks such transfer of useful intelligence.

Public Reputation

Revealing your organization's cyber security vulnerabilities, threats and subsequent risks and perhaps the calculated consequences is very useful intelligence to share with other similar sectors (e.g., via the ISACs) and/or to the government. This may even be viewed as a public duty and patriotic by the entity; however, revealing this information –especially if it is “leaked” as in the Edward Snowden case of 2013³⁷¹– can have financial and reputational consequences.

For instance, the financial markets may “punish” the offending entity through stock sell-offs and bond rating reduction. Additionally, this data may lead to a less than positive reputation for the company by the public, other entities involved in information sharing, and the government.

Although this may appear to be a trivial concern, it is a major issue in the board rooms of all companies globally.

Communications Constraints

An added barrier to information sharing is that there may not be any effective means of communication from one organization under cyber attack to other peer companies. There may not be lists of emails or any portals to post your notice of cyber event. Hence, even if you want to share your cyber related information there may not be a way or means to get the information out to those who could use the data.

Other Barriers

Two other barriers in cyber security information sharing exchanges impacting all critical information sectors are a) denial – there is an issue requiring information sharing for mutual protection, and b) lack of perceived value in spending the resources to share

³⁷¹ Edward Snowden is a former US Central Intelligence Agency ([CIA](#)) employee, and former government contractor who leaked classified information from the United States National Security Agency (NSA) in 2013.

and receive cyber security intelligence. Both of these philosophies of practice have been observed by this author in the industry –including the energy sector– and both can be very difficult to surmount.

These attitudes can be due to lack of knowledge or even a sense of arrogance that the leaders “know all” and cannot be persuaded to participate since it is not a real issue in their minds. Unfortunately, an attack or data breach on the company may result in a change of mind by the executives; however, that is usually too late.

The Biggest Barrier – Lack of Mutual Trust

The largest barrier to all paths of information exchange is the lack of mutual trust by all parties. For instance, the sender may not trust the receiver (e.g. a private company sending sensitive information to the Federal Government). Or, the sender may not trust that the receiver can “adequately control and handle” the sensitive information (e.g. the Federal Government not sharing sensitive intelligence because they simply do not have confidence in the company destined to receive the data).

Overall, this is a large concern and usually the primary reason why intelligence exchanges fail or do not adequately take advantage of this capability.

Trust is not really built between a government and a company, or a company and an ISAC but between individuals. It is critical to break these trust barriers down with face-to-face meetings followed by legal agreements on how the data is handled, stored, destroyed, and released. As observed in the ENISA Good Practice Guide – Network Information Security Information Exchange:

“It is important to establish, and consistently use, codes of practice that minimize the risk of breaches of confidentiality, and increase trust. NDA’s and different levels of information sharing provide members some protection from unauthorized disclosure.”³⁷²

Trust can be achieved but it takes time, dedication and honest exchanges. An example of an information sharing organization at a local level based on trust is the AGORA in the Seattle area. The AGORA was founded over 15 years ago in Seattle, Washington, USA by the then Chief Information Security Officer of the City of Seattle. His vision was to bring together interested and concerned individuals in the Seattle metropolitan area to share ideas and experiences about cyber and physical security threats to their companies and the region’s infrastructure. The AGORA is not affiliated with any government agency and is operated for a very low cost. This approach has been studied and reviewed by cyber security experts in Washington DC, Canada and other international locations.

³⁷² Symantec, and Landitd Ltd, “Good Practice Guide Network Security Information Exchanges”, *ENISA Report*, Athens, Greece, 2009, p.20.

For anyone looking at ways to establish improved trust relationships, a useful resource is an article by Ms. Cynthia Hansen, Head of Professional Services of the World Economic Forum. Her article, entitled “5 Key Lessons on Building Trust in Business”,³⁷³ provides a few key points to consider for ISAC and Information Exchange implementation. The five *misperceptions* she offers are:

- Being compliant is equal to gaining trust – not true, you need to do more than simply follow the rules
- Trust is built through marketing – not true, communication alone must be underpinned by real, authentic action
- A company does not have to be trustworthy to build trust – again, not true. A company that adheres to its values of honesty and doing the right thing, even at the cost of profits, will seem genuine and trustworthy
- The CEO is the face of the organization – do not forget to use all members of the entity/company/team to show that the organization is holistically trustworthy
- Managing trust is managing one’s reputation – it’s best to stay away from “spin” and instead have authentic, direct, honest conversations with the stakeholders.

In summary, Ms. Hansen’s article will offer some ideas –perhaps counterintuitive– on ways to nurture trust in the information exchange/ISAC. Just be sure to recognize that simple display is not the same as demonstration by doing.

Recommendations for Establishing Information-Sharing Mechanism for the Energy Sector

The energy sector globally is extremely vital not only for the resident countries but also for future industrial and technological growth as well as peaceful stability. Of course, cyber attacks should be on the minds of the energy company executives as well as government agencies, energy, commerce and defense sector. Using the US experience with the Electricity-ISAC (E-ISAC), and the ENISA experiences, some recommendations that come to mind include the following:

- Establish an organization or agency that can be viewed as trustworthy and not under the influence or direction of any government organizations that could censor or negatively impact open and honest information sharing.

³⁷³ Cynthia Hansen, “5 Key Lessons on Building Trust in Business”, *World Economic Forum Agenda*, 2015, <https://agenda.weforum.org/2015/10/5-key-lessons-on-building-trust-in-business/>.

- This entity could cover electricity, oil and gas sectors and even the water sector due to its similar infrastructure elements such as pumps, valves, and industrial controls as well as IT systems that could be negatively affected by cyber attacks, worms, viruses, etc.
- This agency could be for one country or for a regional pact. Admittedly the politics of such an arrangement may make a regional pact difficult.
- Establish a rapid communications system that enhances and rapidly announces cyber events, concerns, or good practices to the members of the ISAC or information exchange. This could include such approaches as rapid “text messaging” blasts, daily newsletters, detailed white papers, lessons learned from the region as well as international experiences, etc. These messages from the individual members should still be within certain boundaries of protocol and may permit some anonymity to best protect from accusations of collusion.

Approaches similar to the E-ISAC listed above are highly recommended.

The benefits from this approach could be very substantial and may even encourage cross-sector and cross-border communications regarding common cyber issues. For example, the energy and water sectors use similar industrial controls from common global vendors. If one company identifies cyber issues with a particular device and notifies the ISAC then this information would be useful for the other members even if they are not in the same critical infrastructure sector.

Another benefit is that the newly established ISAC/Information Exchange could become a “think tank” for the country or region relative to cyber security, development of cyber protection and defense policies, and even provide a central location for meetings and training dedicated to cyber defense and policy. One suggestion could also include rotating some of the key staff into the newly established ISAC from the different member companies. Hence, there is improved cross-communications between the different companies; the ISAC knowledge base is strengthened and even more trusted; and, this allows for professional and technical development of the employees who then return to their home companies with better sensitivity and knowledge of cyber security.

Ultimately the biggest benefit hopefully achieved through this idea is the increased cyber safety of the country’s and region’s energy sector from cyber and physical attacks.

Conclusions and the Future

Lack of effective information sharing between the owner/operators of critical infrastructure and the government is not a new issue. It has been happening for many years and was even recognized in the United States in 1998 by the Clinton

Administration with the establishment of the ISACs. Unfortunately, the problem still continues due to legal, financial, and reputational barriers with the penultimate barrier being lack of trust by all parties in the dialogue. As such, until trust and the effective establishment of a true two-way communications flow are foundationally established, the problem with information sharing to protect critical infrastructure will remain.

REFERENCES

BEJTLICH, R., "Sharing Threat Intelligence: Necessary but Not Sufficient?" *Brookings*, 2015. <http://www.brookings.edu/research/testimony/2015/02/02-protecting-america-from-cyber-attacks-information-sharing-bejtlich>.

Bush Administration Staff, "Homeland Security Presidential Directive/HSPD-7." Washington, DC, http://www.isaccouncil.org/images/HSPD_7.pdf, 2003.

CAULEY, G. et al., "Roles of the Electricity Subsector's ISAC and Coordinating Council", Atlanta, GA, http://www.nerc.com/gov/bot/botquarterlyitems/Policy_Input_Package_August_2015_PUBLIC_POSTING.pdf, 2015.

Clinton Administration Staff, *Critical Infrastructure Protection (PDD 63)*, Washington DC: US Executive Branch, <http://fas.org/irp/offdocs/pdd/pdd-63.htm>, 1998.

European Union Agency For Network And Information Security, "Information Sharing" *ENISA Web Page*, <https://www.enisa.europa.eu/activities/cert/support/information-sharing>, 2015.

FAMA, J. P., "Protecting the Electric Grid from Today's Cyber Threats", *Energy Security Forum*, http://www.energybiz.com/magazine/article/433523/protecting-electric-grid-today-s-cyberthreats?inf_contact_key=6a0c50c44fb30c0bdcf215828e473238c4994ca6416fa28d997f354d5dc9ed20, 2015.

FISCHER, E. A., LOGAN, S. M., *Cyber Security and Information Sharing: Comparison of House and Senate Bills in the 114th Congress*, Washington, DC, <https://www.fas.org/sgp/crs/misc/R44069.pdf>, 2015.

George Bush Staff, B. A., "NSIS - Introduction and Overview", *National Strategy for Information Sharing*, Washington, DC, 2007.

GÜCÜYENER, A., "Criticality of Information Sharing for Cyber Security and Models for Energy Sector", Hazar Strategy Institute, Istanbul, Turkey,

http://www.hazar.org/blogdetail/blog/criticality_of_information_sharing_for_cyber_security_and_models_for_energy_sector_1262.aspx, 2015.

HANSEN, C., "5 Key Lessons on Building Trust in Business - Agenda - The World Economic Forum", *World Economic Forum Agenda*, Geneva, Switzerland, <https://agenda.weforum.org/2015/10/5-key-lessons-on-building-trust-in-business/>, 2015.

HAYDEN, E., "Barriers to Information Sharing Negatively Impact Critical Energy Infrastructure Protection", *Energy Security Forum*, No. 8, Vilnius, Lithuania, 2013.

HAYDEN, E., *Infrastructure Security Today Blog*, North Bend, WA, 2013-2015.

HAYDEN, E., "Responses on Cyber Information Sharing for Hazar Strategy Institute" (Private Communication), North Bend, WA, 2015.

MADRIGAL, A. C., "Snipers Coordinated an Attack on the Power Grid, but Why?" *The Atlantic*, <http://www.theatlantic.com/technology/archive/2014/02/snipers-coordinated-an-attack-on-the-power-grid-but-why/283620/>, 2014.

MIELCAREK, K., "Electricity ISAC Renamed, New Portal Launched with Improved Look and Performance", *NERC Webpage*, Atlanta, GA, http://www.nerc.com/news/Headlines_DL/ISAC_Web_24SEP15.pdf, 2015.

MOTEFF, J. D., "Critical Infrastructures: Background , Policy , and Implementation", Washington, DC, <https://www.fas.org/sgp/crs/homesec/RL30153.pdf>, 2015.

NERC STAFF, N. "Electricity ISAC", Atlanta, GA, <http://www.esisac.com>, 2015.

NERC STAFF, N., "E-ISAC - Electricity Sector Information Sharing & Analysis Center" Atlanta, GA, <http://www.esisac.com>, 2015.

NOLAN, A., "Cyber Security and Information Sharing: Legal Challenges and Solutions, Congressional Research Service", Washington DC, <http://www.fas.org/sgp/crs/intel/R43941.pdf>, 2015.

Obama Administration Staff, "Executive Order - Improving Critical Infrastructure Cyber Security", *White House Webpage*, <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>, 2013.

Obama Administration Staff, "Executive Order - Promoting Private Sector Cybersecurity Information Sharing" *White House Webpage*, <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>, 2015.

Obama Administration Staff, "Presidential Policy Directive - Critical Infrastructure Security and Resilience PPD-21", *White House Webpage*,
<https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>, 2013.

PETERSON, D., "CRISP: Market Failure and Fools Gold", *Digital Bond Blog*,
<http://www.digitalbond.com/blog/2014/11/13/crisp-market-failure-and-fools-gold/>,
2014.

ROBERTSON, J., RILEY, M., "Mysterious'08 Turkey Pipeline Blast Opened New Cyber War", *Bloomberg Business*, <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>, 2014.

Security Dispatch, "DOE Enhances Cyber Security Risk Information Sharing Program", *DarkMatters*, <http://darkmatters.norsecorp.com/2014/11/07/doe-enhances-cybersecurity-risk-information-sharing-program/>, 2015.

SILVERSTEIN, K., "Utilities Engaged In Hand-To-Hand Cyber Combat To Keep The Lights On", *Forbes*, <http://www.forbes.com/sites/kensilverstein/2015/09/13/utilities-engaged-in-hand-to-hand-cyber-combat-to-keep-the-lights-on/>, 2015.

SYMANTEC and LANDITD Ltd., "Good Practice Guide Network Security Information Exchanges", *ENISA Report*, Athens, Greece,
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide/at_download/fullReport, 2009.

US Department of Energy, "CRISP-Cybersecurity Risk Information Sharing Program", Washington DC, 2015.

US Department of Homeland Security, "National Infrastructure Protection Plan Information Sharing", Washington, DC, 2007.

US Department of Homeland Security, "National Network of Fusion Centers Fact Sheet", Washington, DC, <http://www.dhs.gov/national-network-fusion-centers-fact-sheet>, 2015.

WEISS, N. E., "Legislation to Facilitate Cyber Security Information Sharing: Economic Analysis", Washington, DC, <https://www.fas.org/sgp/crs/misc/R43821.pdf>, 2014.

THE THREAT OF CYBER TERRORISM – A RISK MANAGEMENT PERSPECTIVE

Marco MACORI

ABSTRACT

After defining the term cyber terrorism, this article outlines a basic cyber terrorism risk management methodology, with a focus on relevant threat actors, i.e. terrorist organizations such as ISIS, and their motivations and capabilities. Furthermore, this article analyzes an alleged cyber terrorism incident with regard to critical energy infrastructure and assesses the likelihood of cyber terrorist attacks in the future.

Key Words: Cyber Terrorism, Risk Management, Threat Assessment, Vulnerability Assessment, Criticality Assessment, ISIS

Introduction

“The greatest risk is a catastrophic attack on the energy infrastructure. We are not prepared for that,” said former NSA director General Keith Alexander, who had led the US defense against cyber threats for many years. General Alexander also recently said the “doomsday” scenario for western countries was coordinated cyber attacks on refineries, power stations, and the electric grid.³⁷⁴ US President Obama has stated that cyber terrorism is perhaps one of today’s greatest threats.³⁷⁵ It is likely that cyber attacks are not only here to stay, but given the increasing reliance on the internet, they are likely to increase significantly. Further work is needed to better understand and assess the risks associated with cyber terrorism – the threats, vulnerabilities, and consequences. Cyber security experts routinely expose vulnerabilities; however, there

³⁷⁴ Ambrose Evans-Pritchard, “NSA veteran chief fears crippling cyber-attack on Western energy infrastructure”, *The Telegraph*, 26 April, 2015, <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11563746/NSA-veteran-chief-fears-crippling-cyber-attack-on-Western-energy-infrastructure.html>

³⁷⁵ Christopher Harress, “Obama Says Cyberterrorism Is Country’s Biggest Threat”, *International Business Times*, 18 February, 2014, <http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337>

is a relative paucity of research on specific cyber terrorism threats and potential consequences. This is problematic, as vulnerability does not equal risk.

Defining Cyber Terrorism

From Terrorism to Cyber Terrorism

Looking back to the 1990s and early 2000s, websites were commonly defaced mostly to satisfy an attacker's ego. Those are examples of cyber vandalism. A more recent example of this sort of attack was the defacement of the US Central Command's Twitter page. However, Stuxnet, discovered in June 2010 and nicknamed the "world's first digital weapon", marked a significant change. Stuxnet had moved beyond the virtual world and was capable of causing physical destruction to computer equipment, perpetrated by nation states against another nation state – an example of cyber warfare. Cyber terrorism seems to have found a different "niche", whereby the destruction or disruption of service does not necessarily have to be a military or state target, but a commercial entity or service.³⁷⁶

Current definitions of cyber terrorism range from narrow to broad, although most experts subscribe to the narrow definition of "pure" cyber terrorism. Barry C. Collin first introduced the term cyber terrorism in the 1980s, although as neither experts nor the United Nations have come to a consensus, there is still no single, unifying definition of cyber terrorism.³⁷⁷ Cyber terrorism is an even more opaque term than terrorism, adding another layer to an already contentious concept. People still tend to use the terms cyber war, cyber terrorism, cyber crime, sabotage, vandalism and hacktivism interchangeably, although there are important differences.

Bruce Hoffman defines terrorism as "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change."³⁷⁸ In order to provide a comprehensive definition of terrorism, the definition must also include that the perpetrator must be a non-state actor (individual or group). If one assumes that this was the accepted definition of terrorism, then the addition of cyber to this term results in a rather simple definition: cyber terrorism is the use of cyber capabilities to commit terrorism. Given the range of cyber terrorism activities described in the literature, this simple definition can be expanded to: "cyber terrorism is the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of

³⁷⁶ Dan Holden, "Is Cyber-Terrorism the New Normal?", *Wired*, <http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/>

³⁷⁷ Barry C. Collin, "The Future of Cyber Terrorism", *Proceedings of the 11th Annual International Symposium on Criminal Justice Issues*, the University of Illinois at Chicago, 1996, p. 3.

³⁷⁸ Bruce Hoffman, **Inside Terrorism**, New York: Columbia University Press, 2006, p. 40.

political change.”³⁷⁹ Cyber terrorism can also include attacks on internet businesses, but when this is done for economic motivations rather than political ones, it is to be regarded as cyber crime. Cyber terrorism is limited to actions by individuals, independent groups, or organizations. Any form of cyber attack conducted by governments and nation states may be defined as cyber warfare.³⁸⁰

FBI Definition of Cyber Terrorism

According to the US Federal Bureau of Investigation (FBI), cyber terrorism is any “premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.”³⁸¹ Unlike a nuisance virus or computer attack that results in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the US Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.³⁸²

“Destructive Cyber Militancy”

The goal of terrorists in using destructive cyber militancy (DeCM) is to manipulate computer code and corrupt information system functions in order to damage or destroy virtual and/or physical assets. Manipulating or corrupting information may, at a minimum, generate misinformation and induce confusion and loss of confidence in critical systems. In the worst case, DeCM may cause catastrophic effects on critical infrastructure, possibly resulting in death and destruction. DeCM activities are often described in the literature as “pure” cyber terrorism, which is the direct use of cyber hardware, software, and networks to create kinetic effects on par with traditional acts of terrorism, as opposed to merely using information communication technology in support of organizational communication and “traditional” terrorism. Most experts in the field narrowly define cyber terrorism to include only the direct use of cyber capabilities, as opposed to activities in support of terrorism.³⁸³

³⁷⁹ Jonalan Brickey, “Defining cyberterrorism – capturing a broad-range of activities in cyberspace”, *CTC Sentinel*, Combating Terrorism Center at Westpoint, 23 August, 2012, <https://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace>

³⁸⁰ Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", *Vanderbilt Journal of Transnational Law*, Vol. 43, No. 1, 14 August, 2009, p. 38.

³⁸¹ Serge Krasavin, “What is Cyber-terrorism?”, *Computer Crime Research Center*, 2001, <http://www.crime-research.org/library/Cyber-terrorism.htm>

³⁸² William L. Tafoya, “Cyber Terror”, *FBI Law Enforcement Bulletin*, November 2011, p. 2.

³⁸³ Ibid. and Sarah Gordon and Richard Ford, “Cyberterrorism?”, *Computers and Security*, 21:7 (2002): pp. 636-647.

Although there have been no destructive cyber terrorism attacks to date, terrorists may engage in DeCM to cause massive physical damage and economic disruption to critical infrastructures such as the power grid, fuel distribution and storage systems, public water sanitation systems, air traffic control systems, and financial systems (especially ATM networks). Many of these critical systems are either directly connected to the internet or indirectly accessible via removable media and out-of-band channels. A 2011 al-Qaida video called upon cyber-savvy mujahidin to attack US critical information systems by conducting an “information raid in the manner of the raids of September 11.”³⁸⁴ The video included translated interviews with US cyber security experts discussing how DeCM-like attacks can cause extensive damage to life-sustaining critical infrastructure. One example of a possible DeCM event would be the destruction of a key natural gas pipeline, the flow of which is regulated by electronic industrial control systems (ICS). These systems are vulnerable to hacking exploits, which could allow for the manipulation of ICS functions such as a sudden increase in pipeline pressure, resulting in a large kinetic explosion.³⁸⁵

“Real Life” Challenges in Defining Cyber Terrorism: The BTC Pipeline Attack

The challenges in categorizing attacks as cyber attacks, and even more so as cyber terrorism, can be effectively illustrated through the following “real life” case: There was a mysterious explosion on the Baku-Tbilisi-Ceyhan (BTC) pipeline in Erzincan/Turkey just before the Russia-Georgia war broke out in 2008. The Turkish government claimed mechanical failure.³⁸⁶ Another explanation at the time was a bombing by the Kurdish PKK terrorist group, and the PKK even claimed responsibility. A pipeline bombing of this sort could indeed fit the attack profile of the PKK, which specializes, among others, in assaults on critical infrastructure. There was widespread speculation that the attack could have been a cyber attack. But the PKK does not have advanced cyber attack capabilities and nor is that their modus operandi. US intelligence officials believed the PKK – which according to leaked US State Department cables has received arms and intelligence from Russia – may have arranged in advance with the (Russian) cyber attackers to take credit. Years later, BP, one of the pipeline construction companies, claimed in documents filed in a legal dispute that it was not able to meet shipping contracts after the attack due to “an act of terrorism.”³⁸⁷

It subsequently emerged that according to US intelligence officials, the chief suspect was Russia: the attack on the BTC pipeline –which follows a route through the former Soviet Union that the US government mapped out over Russian objections– would

³⁸⁴ Al-Shabab, Electronic Jihad Video, 2011, www.hsgac.senate.gov/download/?id=483eca14-3c0e-4a30-9038-f4bf4a1fad60.

³⁸⁵ Brickey, ibid.

³⁸⁶ Jordan Robertson and Michael Riley, “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar”, *Bloomberg*, 10 December, 2014, <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>

³⁸⁷ Ibid.

mark another chapter in the belligerent energy politics of Eurasia. The attack, according to this theory, was the result of a cyber attack on the computers managing the pipeline. Software planted in the pipeline system shut down alarms and raised the pressure in the pipeline to such a high level that it exploded.³⁸⁸ However, and most recently, a leaked internal official inspection report concludes that the explosion was not caused by a cyber operation. Rather, it was a case of “traditional” terrorism using explosives. The assumed cyber attack simply could not have taken place, for various technical reasons.³⁸⁹

Cyber Terrorism Risk Management

In considering terrorism risks, there are a number of underlying elements that go into a risk evaluation:

- What is the risk/threat?
- What are you trying to protect?
- What is the criticality?
- What/who are the potential threat actors?
- What are their intentions/motivation?
- What are their actual/relevant capabilities?
- Where and what are the relevant weaknesses/vulnerabilities?
- What are options to eliminate or mitigate those weaknesses/vulnerabilities?

Risk assessments depend on many multivariate, contextual factors. To lend structure to the assessment, there is the discipline of risk management. Risk management is “a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions that reduce the risk and mitigate the consequences of an attack or event.”³⁹⁰ The methodology acknowledges an important point that is too often disregarded: risk can only be minimized, not eliminated. To lend rigor to the analysis, we try to quantify risk. Thus, risk may be defined mathematically as the probability of the attack occurring multiplied by the probability of success of the attack (or, from another perspective, the inverse probability of failure, interruption, or neutralization) multiplied again by the consequences of the attack (on some arbitrary relative scale).

³⁸⁸ Ibid. and Joshua Kucera, “U.S. Intelligence: Russia Sabotaged BTC Pipeline Ahead of 2008 Georgia War”, *EURASIANET.org*, 10 December, 2014, <http://www.eurasianet.org/node/71291>

³⁸⁹ Hakan Tanriverdi, “Angeblicher Cyberangriff auf Pipeline – Die Tatwaffe fehlt”, *Süddeutsche Zeitung*, 19 June, 2015, <http://www.sueddeutsche.de/digital/tuerkei-ermittler-schliessen-cyberangriff-bei-pipeline-explosion-aus-1.2529345>

³⁹⁰ Raymond J. Decker, “Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts”, *Testimony before the Senate Committee on Government Affairs*, 31 October, 2001, p. 7.

In mathematical terms that is:

$$R = Pa \times Ps \times C$$

Where R is risk; Pa is the probability an attack will be attempted; Ps is the probability of success (or, alternatively 1-Pf, where Pf is the probability of failure); and C is the consequence of the attack.

In other words, terrorism risks represent the expected consequences of attacks, taking into account the likelihood that attacks occur, and that they are successful if attempted. In probabilistic terms, risk from an attack of a certain type is the unconditional expected value of damages of a certain type. There are two advantages of using this formulation of terrorism risk. First, it provides an approach for comparing and aggregating terrorism risk. With this definition, it is possible to compare risks of a specific type across diverse targets. Second, this definition of risk provides a clear mapping between risk and approaches to managing or reducing risk. Intelligence and active defense involving “taking the fight to the enemy” represent an approach to risk management that focuses specifically on threats. Managing risk through vulnerability requires increasing surveillance and detection, hardening targets, or other capabilities that might reduce the success of attempted attacks. Finally, risk can be managed through consequences by increasing preparedness and response, reducing the effects of damage through mitigation or compensation.³⁹¹

Threat Assessment

The probability of an attack includes several separate components. It involves, first, an assessment of near-term threats (based, in part, on current intelligence and an analysis of the adversary's intentions). In other words, we ask, based upon what we know, about the likelihood of a particular individual, asset, location, process, system or function being targeted. We then conduct an evaluation of the adversary's capabilities. What can he accomplish, and with what degree of lethality or impact? Perhaps the biggest change resulting from the terrorist attacks of 9/11 is that we have to fundamentally reassess the adversary's capabilities. This portion of the assessment is called the threat assessment. People or organizations represent a terrorist threat when they have the intent and capability to impose damage to a target. It is essential to note that neither intentions without capabilities nor capabilities without intentions pose a threat per se. Threat only exists when both are manifested together in a person or organization. When the scope of the threat is defined in terms of a specific set of targets, a specific set of attack types, and a specific time period, probability can be used as a measure

³⁹¹ Ibid. and P. Rosenzweig and A. Kochems, “Risk Assessment and Risk Management: Necessary Tools for Homeland Security”, in: *Heritage Backgrounder*, Heritage Foundation, Washington D.C., 25 October, 2005, <http://www.heritage.org/research/reports/2005/10/risk-assessment-and-risk-management-necessary-tools-for-homeland-security> and H. Willis. et al., *Estimating Terrorism Risk: RAND Corporation*, Santa Monica, 2005, pp. 37-45.

of the likelihood that an attack will occur. Thus, we define a measure of threat as follows:

*Measure (Threat): The probability that a specific target is attacked in a specific way during a specified time period.*³⁹²

Vulnerability Assessment

The probability of success (or failure) looks at the other half of the question: what are the vulnerabilities and how can they be mitigated? It involves identifying weaknesses in structures (“cyber structures”), other systems, or processes that could be exploited by a terrorist group. It then seeks to identify the ways to reduce the vulnerabilities identified or, if feasible, to eliminate them.³⁹³ Clearly, not all threats of the same type are equally important. Furthermore, the threat of terrorism is dynamic in that it adapts to current conditions that affect the likelihood of attack success. Therefore, we also need a precise definition of vulnerability that captures information about the infrastructure in which we are interested: vulnerability is the manifestation of the inherent states of the system that can result in damage if attacked by an adversary. To use this definition for measurement, we must be more specific and ask, “vulnerable to what”? Probability can be used as a measure of the likelihood that vulnerability will lead to damage when attacks occur, thus:

Measure (Vulnerability): The probability that damages (where damages may involve fatalities, injuries, property damage, or other consequences) occur, given a specific attack type, at a specific time, on a given target.

In other words, a target’s vulnerability can be articulated as the probability that an attack of a given type will be successful once it has been launched and, as articulated, measures vulnerability to specific types of damages only (i.e., there would be separate vulnerability assessments for deaths, injuries, and property damage). Note that for the measure specified above, magnitude of the damage is not part of the definition of vulnerability. This measure assumes a simplified representation of vulnerability in which there is either a successful attack with damage or no success with no damage. As a result, we define success in terms of whether or not damage, having a distribution of magnitude, is inflicted by the attack.³⁹⁴ Consequence measurement will be discussed below.

Criticality Assessment

The consequences factor is intended to evaluate the effect that will be achieved if the adversary accomplishes his goals. Often the goals will include killing individuals or

³⁹² Rosenzweig/Kochems, Willis et al., Decker: *ibid.*

³⁹³ Rosenzweig/Kochems, Willis et al., Decker: *ibid.*

³⁹⁴ Rosenzweig/Kochems, Willis et al., Decker: *ibid.*

damaging infrastructure, but they may also include social and economic disruption and psychological effects. Not all consequences can be prevented. So in order to assist in prioritization, there is a process designed to identify the criticality of various assets: what is the asset's function or mission and how significant is it? We define consequence as the magnitude and type of damage resulting from successful terrorist attacks. To define a measure of consequence, specificity is again required. In this case, specificity requires treatment of two important considerations: how consequences are measured and how uncertainty is addressed. Formally, we state this as follows:

Measure (Consequence): The expected magnitude of damage (e.g., deaths, injuries, or property damage), given a specific attack type, at a specific time, that results in damage to a specific target.

Consequences can be expressed in terms of fatalities, injuries, economic losses, or other types of damage. Other aspects of consequences can also be considered using the approach outlined here.³⁹⁵

Exemplary Evaluation of a Cyber Threat Actor: So-called “Islamic State” (or ISIS)

Over the past years, ISIS and pro-ISIS hackers, as well as hackers claiming to be associated with or operating in the name of ISIS, have been conducting cyber attacks around the world. The targets have included media outlets, government agencies, universities, NGOs, and businesses. During this time, there has also been a debate regarding ISIS' cyber capabilities, about whether it seeks to wage “cyber jihad” against the West, and about the hacking capabilities of its members and online supporters. While some cyber security analysts have attempted to downplay the significance of these attacks by ISIS and pro-ISIS elements, and by others claiming an ISIS affiliation, the issue of cyber attacks by ISIS elements is being taken very seriously by governments and law enforcement.³⁹⁶ For instance, the FBI warned in a Public Service Announcement titled “ISIL Defacements Exploiting WordPress Vulnerabilities” on April 7, 2015, that “continuous Web site defacements are being perpetrated by individuals sympathetic to the Islamic State in the Levant (ISIL), a.k.a. Islamic State of Iraq and Al-Sham (ISIS). The defacements have affected website operations and the communication platforms of news organizations, commercial entities, religious institutions, federal/state/local governments, foreign governments, and a variety of other domestic and international websites. Although the defacements demonstrate low-level hacking sophistication, they are disruptive and often costly in terms of lost

³⁹⁵ Rosenzweig/Kochems, Willis et al., Decker: *ibid.*

³⁹⁶ S. Stalinsky and R. Sosnow, “Hacking In The Name of The Islamic State (ISIS)”, *MEMRI*, 21 August, 2015, <http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html>

business revenue and expenditures on technical services to repair infected computer systems.”³⁹⁷

FBI director James Comey added, at the Cyber Security Law Institute at Georgetown University in May 2015, that ISIS was “waking up” to the idea of initiating a cyber attack against critical US infrastructure with sophisticated malware. “Logic tells me it’s coming,” said Comey, adding that ISIS is “looking into” whether it would be capable of perpetrating such attacks. Over the last two years, he said, there has been more attention paid to potential cyber attacks against the US, and although he has not seen them yet, “it just makes too much sense” that destructive malware would end up in the hands of terrorists. “Destructive malware is a bomb, and terrorists want bombs.”³⁹⁸

In the most recent significant hack, on August 11, 2015, the Islamic State Hacker Division (ISHD) released what it claimed was a large collection of names, emails and other sensitive information belonging to US military and government personnel. Earlier this year, in March, the same group had “doxxed” 100 US military personnel, and, in May 2015, Italian military personnel – tweeting “hit lists” that included personal addresses, phone numbers, and photos. By posting such information, ISIS and pro-ISIS hackers are facilitating – and even encouraging – “lone wolf” terrorism attacks on these individuals.³⁹⁹

It should be noted, however, that some of the aforementioned cyber operations may not have been perpetrated by ISIS after all. For instance, during a recent cyber security conference in Berlin/Germany the president of the German domestic intelligence service BfV, H. G. Maaßen, floated the theory that the ISIS cyber attack on the French TV channel TV5 Monde in April of 2015 may very well have been a “false-flag” operation by the Russian government – aimed at diverting attention from Russia’s illegal military operations in Ukraine.⁴⁰⁰ Whether or not this theory is ultimately proven correct, it illustrates the complex, critical issue of reliable attribution and, therefore, of producing actionable intelligence in the context of cyber attacks.

Conclusion

Cyber terrorism is most certainly an attractive option for “modern” terrorists, who value its anonymity, potential to inflict massive damage, psychological impact, and media appeal. However, fears of cyber terrorism have sometimes been exaggerated. Cyber attacks on critical components of the national (energy) infrastructure are not uncommon, but they have not yet been conducted by terrorist groups and have not

³⁹⁷ Ibid.

³⁹⁸ Ibid.

³⁹⁹ Ibid.

⁴⁰⁰ Johannes Leithäuser, “Aufrüstung für den Krieg der Zukunft”, *Frankfurter Allgemeine Zeitung*, 18 September, 2015, p. 4.

sought to inflict the kind of damage that would qualify as cyber terrorism. For the case of cyber terrorism, we must consider the use of cyber attacks in the context of the political goals and motivations of terrorist groups, and whether cyber attacks are likely to achieve these goals. On a national level, where hundreds of different systems provide critical infrastructure services, failure is a fairly routine occurrence at the system or regional level. Cyber terrorists would need to attack multiple targets simultaneously for long periods of time to create “real” terror or achieve strategic political goals. For much of the critical (energy) infrastructure, multiple sustained, effective attacks are not a very likely scenario for terrorist groups – at least at this point. But although the fear of cyber terrorism may sometimes be manipulated and exaggerated by vested interests, we should, of course, neither deny nor ignore it.

Paradoxically, success in the “fight against terrorism” is likely to make terrorist groups turn increasingly to unconventional weapons, such as cyber attacks. For terrorist groups, cyber-based attacks have distinct advantages over physical attacks: they can be conducted remotely, anonymously, and relatively cheaply, and they do not require significant investment in weapons, explosives and personnel. The effects can be widespread and profound. Thus, incidents of cyber terrorism are likely to increase in the future. They will be conducted through denial of service attacks, malware, and other methods that are difficult to envision today. In an article about cyber attacks by Iran and North Korea, the New York Times once observed, “The appeal of digital weapons is similar to that of nuclear capability: it is a way for an outgunned, outfinanced nation to even the playing field.”⁴⁰¹ The same rationale would perfectly fit the cost-benefit-analysis and modus operandi of terrorist groups.

REFERENCES

AL-SHABAB, *Electronic Jihad Video*,

www.hsgac.senate.gov/download/?id=483eca14-3c0e-4a30-9038-f4bf4a1fad60, 2011.

BRICKEY, J., “Defining Cyber Terrorism – Capturing a Broad-Range of Activities in Cyber Space”, *CTC Sentinel*, Combating Terrorism Center at Westpoint, 23 August 2012, <https://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace>

⁴⁰¹ Nicole Perlroth and David E. Sanger, “Cyberattacks Seem Meant to Destroy, Not Just Disrupt”, *The New York Times*, March 28, 2013, <http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html>

COLLIN, B. C., "The Future of Cyber Terrorism", *Proceedings of the 11th Annual International Symposium on Criminal Justice Issues*, the University of Illinois at Chicago, 1996.

DECKER, R. J., "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts", Testimony before the Senate Committee on Government Affairs, October 31, 2001.

EVANS-PRITCHARD, A., "NSA Veteran Chief Fears Crippling Cyber-Attack on Western Energy Infrastructure", *The Telegraph*, April 26, 2015,
<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11563746/NSA-veteran-chief-fears-crippling-cyber-attack-on-Western-energy-infrastructure.html>

GABLE, K. A., "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", *Vanderbilt Journal of Transnational Law*, Vol. 43, No. 1, August 14, 2009.

GORDON, S. and FORD, R., "Cyberterrorism?", *Computers and Security*, 21:7, 2002.

HARRESS, C., "Obama Says Cyberterrorism is Country's Biggest Threat", *International Business Times*, 18 February 2014,
<http://www.ibtimes.com/obama-says-cyberterrorism-countrys-biggest-threat-us-government-assembles-cyber-warriors-1556337>

HOFFMAN, B., **Inside Terrorism**, New York: Columbia University Press, 2006.

HOLDEN, D., "Is Cyber-Terrorism the New Normal?", *Wired*,
<http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/>

KRASAVIN, S., What is Cyber-terrorism?, Computer Crime Research Center,
<http://www.crime-research.org/library/Cyber-terrorism.htm.K>, 2001.

UCERA, J., "U.S. Intelligence: Russia Sabotaged BTC Pipeline Ahead of 2008 Georgia War", *EURASIANET.org*, 10 December, 2014,
<http://www.eurasianet.org/node/71291>

LEITHÄUSER, J., "Aufrüstung für den Krieg der Zukunft", Frankfurter Allgemeine Zeitung, 18 September 2015.

PERLROTH, N. and SANGER, D. E., "Cyber Attacks Seem Meant to Destroy, Not Just Disrupt", *The New York Times*, 28 March 2013,

<http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html>

ROBERTSON, J. and RILEY, M., "Mysterious'08 Turkey Pipeline Blast Opened New Cyberwar", *Bloomberg*, 10 December 2014,
<http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>

ROSENZWEIG, P. and KOCHEMS, A., "*Risk Assessment and Risk Management: Necessary Tools for Homeland Security*" Heritage Backgrounder, Heritage Foundation, Washington D.C., 25 October 2005,
<http://www.heritage.org/research/reports/2005/10/risk-assessment-and-risk-management-necessary-tools-for-homeland-security>

STALINSKY, S. and SOSNOW, R., "Hacking In The Name of the Islamic State (ISIS)", *MEMRI*, 21 August 2015, <http://www.memrijtm.org/hacking-in-the-name-of-the-islamic-state-isis.html>

TAFOYA ,William L., "Cyber Terror", **FBI Law Enforcement Bulletin**, November 2011.

TANRIVERDI, H., "Angeblicher Cyberangriff auf Pipeline – Die Tatwaffe fehlt", *Süddeutsche Zeitung*, 19 June 2015,
<http://www.sueddeutsche.de/digital/tuerkei-ermittler-schliessen-cyberangriff-bei-pipeline-explosion-aus-1.2529345>

WILLIS, H. et al., "Estimating Terrorism Risk", *RAND Corporation*, Santa Monica, 2005.

NUCLEAR ENERGY AND CYBER SECURITY DOMAIN AT CROSSROADS IN DIGITAL TECHNOLOGIES NEW PHASES

Prof. Dr. Mesut Hakkı CAŞIN

ABSTRACT

Energy is a part of the modern society. But we should ask: how can we break ourselves free from dependence on fossil resources and how can we manage to prevent global warming to save our future? One important answer to these critical questions would be the use of advanced and secure nuclear technology for meeting current energy demand and future energy needs without emitting carbon dioxide and other atmospheric pollutants. Indeed, nuclear power plants provided 12 percent of all of the world's electricity production in 2014. Basically, if this energy gap is not filled, the state's energy power capacity may not be able to cover the population's electricity requirements.

There have been three major reactor accidents in the history of civil nuclear power - Three Mile Island, Chernobyl, and Fukushima. However, the evidence over six decades shows that nuclear power is a safe means of generating electricity. In that regard, this article examines and explains the immediate need for revised nuclear energy security operations as well as the current operations underway to address these concerns.

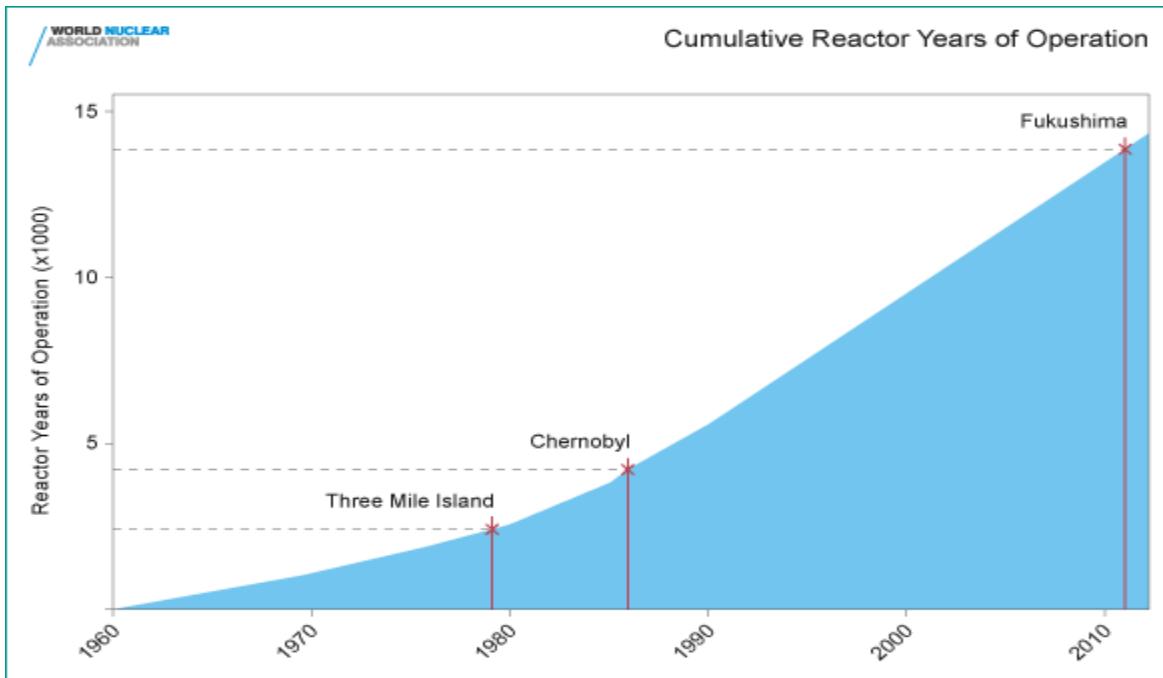
Key Words: Nuclear Energy, Safety, Security, Nuclear Power Plants, Cyber Security, Cyber Terrorism

Understanding General Safety and Security Mentality of Nuclear Facilities

In the 21st century, we can observe that nuclear energy industry has been seen at different times from various perspectives in daily life of modern societies. But beyond the Chernobyl and Fukushima nuclear disasters, there are serious emerging concerns in the international community about the health hazards of radiation. Safety and security measures have been developed in order to prevent possible catastrophic disasters in the future. The operation of nuclear power plants (NPPs) has been investigated in the aspect of safeguard assessment. The risk of terror in NPPs is one of the critical points in secure power operations. Considering the increasing importance of security, there is a vital need to safeguard power plants for reliable electricity

production. Life extensions of nuclear power plants (NPPs) have been performed after the safety evaluation for the plant in order to meet the electricity demand and to save on construction costs due to the aged systems of NPPs. Serious attacks like terror attacks or sabotage are not notified before the incidents.⁴⁰²

Below is a table showing all reactor accidents and listing some energy-related accidents with multiple fatalities.⁴⁰³



Source: http://g.foolcdn.com/editorial/images/143982/cumulative-reactor-years_crop_large.jpg

The 2008 global economic recessions slowed the growth of electricity demand. And in March 2011, an earthquake and tsunami knocked out power at the Fukushima Daiichi Nuclear Plant in northern Japan, causing partial meltdowns at the plant's three active reactors and large-scale releases of radioactive steam.

Nuclear power has been used to produce electricity since the early 1950s. Today there are more than 430 nuclear power reactors, with a total capacity of about 372 gigawatts

⁴⁰² T.-H. Woo: "Nuclear Safeguard Protocol (NSP) Construction of Energy Policy in Nuclear Power Plants (NPPs) for Secure Power Production", *Energy Sources*, 2015, Part B, Vol. 10, No.1, 2015, p. 91–102.

⁴⁰³ Three Mile Island (USA 1979) where the reactor was severely damaged but radiation was contained and there were no adverse health or environmental consequences.

Chernobyl (Ukraine 1986) where the destruction of the reactor by steam explosion and fire killed 31 people and had significant health and environmental consequences. The death toll has since increased to about 56. Fukushima (Japan 2011) where three old reactors (together with a fourth) were written off and the effects of loss of cooling due to a huge tsunami were inadequately contained.

electric (GWe), operating in 30 countries plus Taiwan. An additional 70 units, totaling more than 60 GWe, are under construction. During 2011, nuclear power produced more than 2.5 trillion kilowatt-hours (kWh) of electricity. Globally, the nuclear energy industry now has about 15,000 reactor-years of operating experience. The contribution of nuclear energy to total electricity generation varies considerably from country to country and in different parts of the world. In Western Europe, nuclear-generated electricity accounts for almost 27 percent of total electricity supply. In both North America and Eastern Europe, it is approximately 18 percent. In the Far East, nuclear energy accounts for 10 percent of electricity generation, whereas in Africa and Latin America it is 2.1 percent and 2.4 percent, respectively. In the Middle East and South Asia, it accounts for just 1 percent. As shown above, nuclear energy use is concentrated in technologically advanced countries.⁴⁰⁴

Security at nuclear power plants is a highly important issue for modern communities in almost every state. Of course, a full-scale meltdown of a major reactor would be a big accident and it may have devastating environmental results. In spite of ongoing critical nuclear negotiations in 2010, the Stuxnet⁴⁰⁵ cyber attack was designed to be a significant threat to the Iranian nuclear program by targeting Natanz nuclear plant facilities. Nearly three dozen states have relied on nuclear power plants to meet their energy needs over the last five decades. Since the 2000s, many countries have expressed a newfound interest in civilian nuclear development as part of the so-called “nuclear energy renaissance”.⁴⁰⁶ In modern and civilized community’s daily life, nuclear energy industry has been identified as one of the most highly regulated and safest industries in the world which takes cyber⁴⁰⁷ threats seriously; as one of the urgent and complex challenge. We know well that nuclear power facilities use digital and analog systems to monitor, operate, control, and obtain and store vital information. States are

⁴⁰⁴ “Restoring U.S. Leadership in Nuclear Energy- A National Security Imperative”, The CSIS Commission on Nuclear Energy Policy in the United States, A National Security Imperative, June 2013,

http://csis.org/files/publication/130614_RestoringUSLeadershipNuclearEnergy_WEB.pdf

⁴⁰⁵ *First instance of a computer network attack known to cause physical damage across international boundaries.*

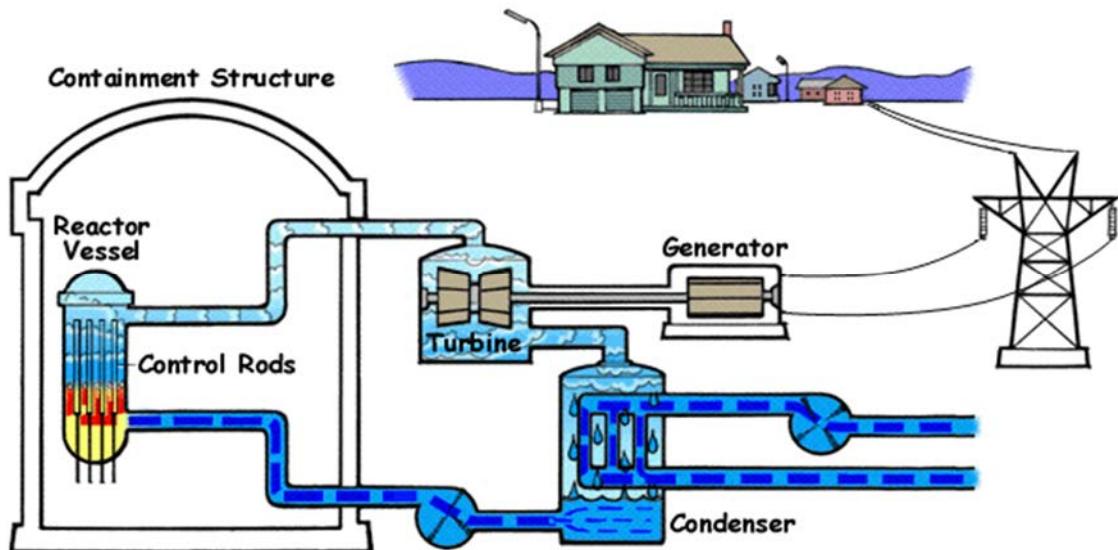
⁴⁰⁶ Matthew Fuhrmann, “Splitting Atoms: Why Do Countries Build Nuclear Power Plants?”, *International Interactions*, Vol.35, No.1, pp. 22-57.

⁴⁰⁷ Cyber is a prefix standing for computer- and electromagnetic spectrum related activities, and the cyber domain includes not only the Internet of networked computers but also intranets, cellular technologies, fiber optic cables, and space-based communications. This domain is a complex man-made environment in which the barriers to entry are so low that non-state actors and small states can play significant roles. Analysts of cyber space are still not clear about the meaning of offense, defenses, deterrence, escalation, norms, and arms control. At the same time, there is a danger of hyping the cyber threat. Joseph S. Nye, Jr., “From bombs to bytes: Can our nuclear history inform our cyber future?”, *Bulletin of the Atomic Scientists*, Vol.69, No.5, September/October 2013,
<http://thebulletin.org/2013/september/bombs-bytes-can-our-nuclear-history-inform-our-cyberfuture>, (Accessed on 01.08.2015), pp. 8-14.

under the responsibility of protecting their nuclear plants.⁴⁰⁸ In spite of many advantages, increasing use of digital systems may be infected or modified by a virus, third-party code developers, or unauthorized breaches from the Internet. After the attacks of September 11, 2001 the nuclear energy industry has begun to address cyber security. Nuclear power plants may be vulnerable to cyber attacks by terrorist organizations. In the post-Cold War period, cyber era is widely dispersed and cyber terrorists as a new phenomenon have been emerged. The following questions should be put forward in order to better understand this phenomenon:

- Are there some small but effective Achilles' Heels within the plants for cyber attacks by the terrorist organizations? Why do countries build nuclear power plants?
- What kind of reasonable steps we can take to improve security at nuclear power plants?
- Does the diffusion of nuclear programs encourage nuclear terrorism?
- With cyber attacks and terrorist threats coming from every destination of the globe, how can a state and international organization find the reliable security systems and the expertise to implement measures for protecting nuclear power plants?
- How do the nuclear energy and cyber security domains interact at crossroad that what are the policy implications of these interactions going forward?

⁴⁰⁸ We must remember that all our nuclear power plants are old and decades ago, the controls of all nuclear power plants were completely analog. Analog systems do their job by following "hard-wired" instructions, while digital computer-based systems follow instructions (software) stored in memory. In addition, many plant computer systems are now linked to digital networks that extend across the plant, performing safety, security and emergency preparedness functions. Protecting these critical digital assets and the information they contain from sabotage or malicious use is called cyber security. Today, digital systems monitor the critical operating conditions (valve openings, pump status, temperatures, pressures, levels, radiation, loading, etc.) of most nuclear plants, while they are still controlled by analog controls.



Source: <http://www.ucsusa.org/sites/default/files/images/2015/08/np-how-Boiling-Water-Reactor-works.gif>

Nuclear security is the protection of nuclear material, other radioactive material, associated facilities, and associated activities, including transport security.⁴⁰⁹ Nuclear security measures are designed to support the prevention of, detection of, and response to, criminal or intentional unauthorized acts such as theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving or directed at materials, facilities or operations. Physical security at nuclear power plants involves the threat of radiological sabotage –a deliberate act against a plant that could directly or indirectly endanger public health and safety through exposure to radiation.⁴¹⁰ Security of nuclear plants requires a multilayered approach, referred to as “defenses in depth”. Nuclear plant security measures are designed to protect three primary areas of vulnerability:

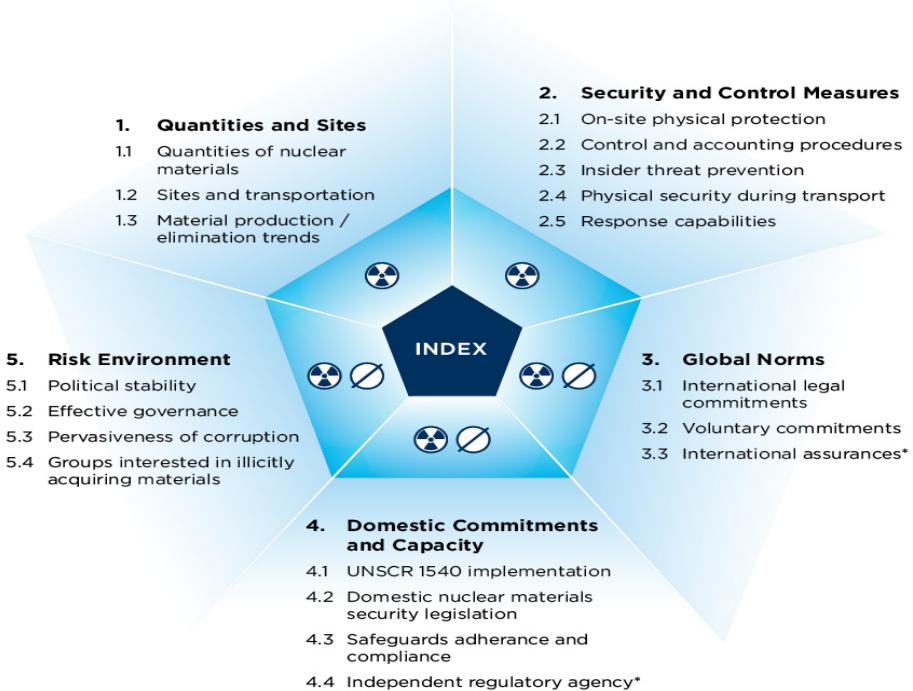
- Controlling the nuclear chain reaction,
- Cooling systems that prevent hot nuclear fuel from melting even after the chain reaction has stopped, and
- Storage facilities for highly radioactive spent nuclear fuel.⁴¹¹

⁴⁰⁹ Donald D. Dudenhoeffer, “Office Of Nuclear Security Cyber Security Programme”, *International Atomic Energy Agency*, https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf, and “Computer Security at Nuclear Facilities - IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual”, 2011, http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf, (Accessed on 24.08.2015).

⁴¹⁰ Mark Holt, Anthony Andrews, “Nuclear Power Plant Security and Vulnerabilities”, *Congressional Research Service*, 3 January 2014, <https://www.fas.org/sgp/crs/homesec/RL34331.pdf>, (Accessed on 01.08.2015).

⁴¹¹ Nuclear facilities could improve safety-security in technical ways, including more secure emergency electrical supplies, better security for control rooms, and, at new plants, reactor

The plant sites are divided into three zones: an “owner controlled” buffer region, a “protected area,” and a “vital area.” Access to the protected area is restricted to a portion of plant employees and monitored visitors, with stringent access barriers. The vital area is further restricted, with additional barriers and access requirements.



Source: http://ntiindex.org/wp-content/uploads/2014/01/How_the_NTI_Index_Measures_Nuclear_Security_Conditions1.jpg

Nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events. But deliberate attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not analyzed when design requirements for today's reactors were determined. Nuclear industry spokespersons have countered by pointing out that relatively small, low-lying nuclear power plants are difficult targets for attack, and have argued that penetration of the containment is unlikely and that even if such penetration occurred it probably would not reach the reactor vessel. Fires and explosions caused by an aircraft crash outside the reactor containment could disable systems required to cool the reactor core and spent fuel pools.⁴¹²

containment structures built to survive attacks by terrorist-flown airplanes. At the institutional level, regulators could strengthen the safety-security interface by requiring that it be built into the life cycle of nuclear plants, from design to dismantlement.

⁴¹² Strengthening the safety-security interface will be a complex undertaking. Systems that prevent and respond to nuclear accidents and nuclear terrorism must be improved and, where they overlap, made to work seamlessly with one another. They must also take into

Due to the dependency of modern societies on cyber technology, cyber security has become a number one state priority. Perhaps one of the most serious threats facing states is the use of cyber capabilities to conduct military-style operations with the aim of degrading, denying or destroying information resident on computers or computer networks.⁴¹³ We think that with the emergence of high sped electronic innovations and IT methodologies such as social media, connection between general cyber space safety and modern states' national security that is often presented as an unquestionable and uncontested academic "truth. It should be emphasized that in the cyber domain, nuclear power plants are considered among the most vital critical infrastructure assets and therefore in need of additional security. In this regard, nuclear power plants are required to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Offensive cyber capabilities pose serious security challenges, especially in the nuclear domain. While the probability of a release of radioactive material through a combined physical and cyber attack on nuclear assets is relatively low, the consequences could be devastating. Awareness of these vulnerabilities is growing, leading states to develop and implement strategies for preventing and managing dangerous cyber incidents.⁴¹⁴ Today and in the near future, rapid changes in high-technology with operational devices is really causing the critical infrastructure facilities of the energy industry to broaden its spectrum of possible threats that can get an attack from almost any place now.⁴¹⁵

During the early years of commercial nuclear power development in the 1950s and 1960s, the main concern with regard to reactor safety was the possibility of a severe accident that would cause a massive release of radioactivity into the environment.⁴¹⁶ Modern nuclear plants can run for long periods between closures for maintenance or refueling, and the raw material for nuclear fuel is relatively abundant and inexpensive

account a third type of possible nuclear catastrophe: the combined disaster, in which opportunistic antagonists time their malicious activity to take advantage of natural disasters that weaken nuclear safety systems.

⁴¹³ Nils Melzer, "Cyberwarfare and International Law", *UNIDIR Resources*, 2011, <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>, (Accessed on 02.08.2015).

⁴¹⁴ Vincent Boulain and Tanya Ogilvie-White, "Cyber Threats and Nuclear Dangers", Asia Pacific Leadership Network for Nuclear Non-Proliferation and Disarmament, *Centre for Nuclear Non-Proliferation and Disarmament, Policy Brief*, No. 17, November 2014, <http://www.a-pln.org/sites/default/files/apln-analysis-docs/Policy%20Brief%20No%2017%20-%20Cyber%20Threats%20and%20Nuclear%20Dangers.pdf>, (Accessed on 02.08.2015).

⁴¹⁵ In 2011, China-based hackers targeted international oil and energy companies in cyberattacks dubbed "night dragon" Laura Baron Lopez, "Cyber threats put energy sector on red alert", *The Hill*, 15 July 2014, <http://thehill.com/policy/energy-environment/212220-cyberthreats-put-energy-sector-on-red-alert>, (Accessed on 02.08.2015).

⁴¹⁶ J. Samuel Walker, "Regulating against Nuclear Terrorism: The Domestic Safeguards Issue, 1970-1979", *Technology and Culture*, Vol. 42, No. 1, January, 2001, pp. 107-132.

compared with fossil fuels.⁴¹⁷ Nuclear and related facilities largely rely on hardware, software and network systems to ensure their daily operation as well as the physical security of the facility. A cyber attack on a nuclear facility could potentially impact the nuclear safety and security of the facility, resulting in the theft of nuclear material or in a nuclear incident with potential risk of release of radioactivity into the atmosphere.⁴¹⁸ The nuclear power plant operating and technical support staff all use computer networks, and connections may exist between these systems and plant control systems. If the hardware or software used is modified or replaced, the reactor might be forced into an accident and the emergency response systems may fail to prevent disasters. With this in mind, there will be a need to consider the current nuclear security framework and where elements of cyber security can and should appropriately be operated.

Nuclear Safety and Design Basis Threat

The nature and strength of the protection provided by each enforcement policy differs. There is an overestimated benefit in maintaining design secrets when it comes to ensuring security. When analyzing the language directly from the rule, there are three distinct groups or types of requirements:

- Performance Requirements,⁴¹⁹
- Programmatic Requirements⁴²⁰ and

⁴¹⁷ "Answering the big questions about new nuclear power stations", *EDF Energy*, <http://www.edfenergy.com/energyfuture/edf-energys-approach-why-we-choose-new-nuclear/implications-for-new-nuclear>, (Accessed on 02.08.2015).

⁴¹⁸ Denis Flory, "International Conference Cyber Space, Energy & Development: Protecting Critical Energy Infrastructure ITU Headquarters, Geneva", 10 October 2014, <http://www-ns.iaea.org/downloads/coordination/ddg/2014/itu-geneva-10oct2014.pdf>, (Accessed on 02.08.2015).

⁴¹⁹ High-level description, Provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat. Specific requirements: • Protect digital computer and communication systems and networks associated with safety related and important-to-safety functions, security functions, emergency preparedness (SSEP) functions, including offsite communications; and support systems and equipment which, if compromised, would adversely impact SSEP functions • Protect the systems and networks from cyber attacks that would adversely impact the integrity or confidentiality of data and/or software, deny access to systems, services, and/or data and adversely impact the operation of systems, networks, and associated equipment • Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks • Ensure that appropriate facility personnel, including contractors are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities • Evaluate and manage cyber risks • Ensure that modifications to assets are evaluated before implementation to ensure cyber security performance objectives are maintained.

⁴²⁰ High-level description: Establish, implement, and maintain a cyber security program. Specific requirements: • Implement security controls to protect the identified assets from cyber attacks • Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks • Mitigate the adverse effects of cyber attacks • Ensure that the functions of protected assets are not adversely impacted

- Documentary Requirements⁴²¹ that the cyber security program must meet.

Security measures include:

- Physical barriers, electronic detection and assessment systems, and illuminated detection zones,
- Electronic surveillance and physical patrols of the plant perimeter and interior structures,
- Bullet-resisting protected positions throughout the plant,
- Robust barriers to critical areas,
- Background checks and access control for employees, and
- Highly trained, well-armed security officers.

However, basically, the cyber attacks can originate from external and internal sources –and as electronic defenses improve, the development of cyber attack tools keeps pace. In 1999, the IAEA introduced a new concept for nuclear facility security, the design-basis threat, defining it as the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated. Design-basis threats are based on real threats and threat scenarios, but they clearly do not cover all contingencies. For example, the IAEA's primary methods for defending against a design-basis threat are aimed at countering ground attacks on nuclear facilities but do not take into consideration the possibility of aerial attacks. In the post-Fukushima era, the scope of design-basis threats should be reconsidered. Since a design-basis threat is considered the maximum credible threat, the scope of these threats should also be broadened to cover the entire spectrum of possible

by cyber attacks • Review the cyber security program as a component of the physical security program in accordance with the requirements of the physical security program.

⁴²¹ High-level description, Develop and maintain a cyber security plan (CSP) and supporting technical documentation. Specific requirements: • Develop and submit a CSP with implementation schedule for review and approval • Establish and maintain a CSP that implements the cyber security program requirements • The CSP must describe how requirements are met and account for site-specific conditions • Develop and maintain written policies and procedures to implement the CSP • The CSP must include measures for cyber incident response and recovery • The CSP must include measures for timely detection and response to cyber attacks • The CSP must include measures for the mitigation of the consequences of cyber attacks • The CSP must include measures to correct exploited vulnerabilities • The CSP must include measures for restoring affected systems, networks, and/or equipment resulting from a cyber attack • Retain all records and supporting technical documentation as a record until the Commission terminates the license for which the records were developed, and maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission. Perry Pederson, "Regulating Nuclear Cyber Security: The Core Issues: An analysis of existing regulatory frameworks in light of the increasing cyber threat against critical infrastructure", *The Langner Group Washington DC*, January 2015, <http://www.langner.com/en/wp-content/uploads/2015/01/Regulating-Nuclear-CyberSecurity.pdf>, (Accessed on 03.08.2015).

terrorist attacks, as is the case with severe accident scenarios for a design basis accident.⁴²² Technical measures to strengthen nuclear safety-security at nuclear facilities will depend on the specific characteristics of the facilities. But all nuclear plant operators and regulators should consider the following measures to strengthen⁴²³ nuclear safety-security:

- Secure the electrical supply,
- Protect the reactor cooling system,
- Make spent fuel ponds safer,
- Guard the main control room, and
- Strengthen the containment structure.

⁴²² For those with malicious intent, who wanted to sabotage a nuclear power plant and release radiation, they would need knowledge about the plant's safety systems, including its power supplies and cooling equipment. Such information is not easily obtainable, but well prepared terrorists particularly those with connections to people working at a nuclear plant could likely acquire it. It is possible to imagine terrorists marrying such information with the safety weaknesses exposed by the Fukushima catastrophe and targeting spent nuclear fuel or core cooling systems at other nuclear plants. In other words, Fukushima has implicitly exposed the relationship between the nuclear safety problem and the nuclear security problem. The disaster also suggests that nuclear power plant safety and security can be strengthened simultaneously through improvements in vital areas, including on-site power supplies, the cooling system for reactors and spent fuel ponds, and the main control room. See, Duyeon Kim, Jungmin Kang, "Where Nuclear Safety and Security Meet", *Bulletin of the Atomic Scientists*, 2012, Vol. 68, No. pp. 86–93.

⁴²³ The fundamental reason for the Fukushima nuclear accident was a prolonged station blackout caused by the failure of off- and on-site sources of **electric power**. Off-site power lines are, generally speaking, outside the control of nuclear plant operators. So security for on-site back-up power sources usually diesel generators needs to be strengthened to protect them from terrorist attack. Emergency generators should be located on high ground to prevent the kind of flooding that disabled back-up power at Fukushima. In case either natural or human activity disables emergency generators, nuclear plant operators should ensure ready access to mobile emergency generators sufficient to power all plant cooling systems. **Operators need to enhance security** to protect reactor cooling pumps and controls from sabotage. Plant operators should also create an on-site water reservoir that can be used to remove decay heat from reactor fuel in the event cooling pumps fail or are sabotaged. The Fukushima accident shows that **spent fuel storage pools are vulnerable** when cooling systems fail. Protection of the pools should, therefore, be part of a nuclear plants safety-security plan, and plant operators should have sufficient water reserves on site to cool the pools, even if a natural disaster or sabotage damages them. To minimize risks in this area, plant operators should move spent fuel from the pools after five years of cooling and place it in dry-cask storage. **Destruction of the main control room** by, for example, a terrorist bomb would cause unpredictable results, including, perhaps, core meltdown. Therefore, plant operators should double the physical security dedicated to the main control room. New reactors need to include **improved protection against aircraft** crashes. A robust containment structure could protect a reactor against a large, terrorist-flown aircraft, preventing or limiting what would otherwise be a significant release of radioactive material. Duyeon Kim, Jungmin Kang, ibid.

Cyber Terrorism Threat against Nuclear Facilities

"For the foreseeable future, acts of cyber terrorism, such as the ones usually imagined, will be very difficult to perform, unreliable in their impact, and easy to respond to in relatively short periods of time."

Douglas Thomas⁴²⁴

Computers control everything in our everyday life and activities (temperature in our home, outdoor lights, our cars, traffic lights, elevators, parking etc.). Even critical national infrastructure is also dependent on control by computers. All of these computers could be potentially hacked or infected by malware.⁴²⁵ Computer systems assist to operate nuclear power plants and it is considered that safety equipment are isolated from the internet and from internal computer networks to protect them against possible outside cyber attacks. Today, cyber security is a highly important input of a state's security, but needs international cooperation since their protection from cyber attacks against critical infrastructures is closely related the competitiveness of the

⁴²⁴ Ronald L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation

Before the House Committee on Governmental Reform, Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee Washington, DC, 24 June 2002, <https://www.fbi.gov/news/testimony/cyberterrorism-and-critical-infrastructure-protection>, (Accessed on 03.08.2015).

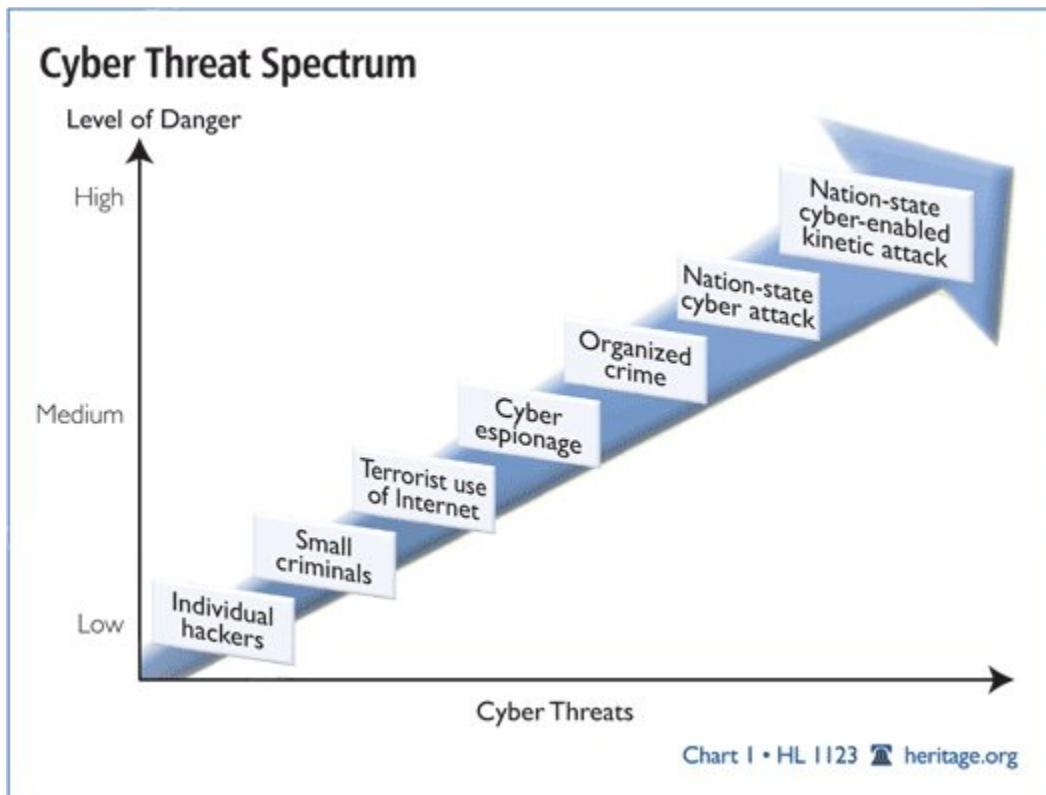
⁴²⁵ Over the past half-century, digital technology has become deeply embedded in the fabric of political and economic life. Networked computers underwrite the performance of the global financial system, industrial services and manufacturing, public utilities and government bureaucracy, and military surveillance and power projection. Systems that connect organizations across borders and automate routine processes have greatly improved operating efficiency over the long run. Cyber warfare, in contrast with all of the above, employs computer network attacks as a use of force to disrupt an opponent's physical infrastructure for political gain. This includes military cyber operations that degrade enemy data processing to facilitate an integrated assault during wartime. Such tactical measures are a functional outgrowth of the electronic warfare tradition, as exemplified in the 2007 Israeli airstrike on a Syrian reactor that may have relied on cyber attacks to blind Syrian radars.

David A. Fulghum, "Why Syria's Air Defences Failed to Detect Israelis," *Aviation Week*, Ares Blog,

3 October 2007. Some sources dispute whether the Israelis used cyber attack or more traditional forms of electronic jamming; Ellen Nakashima, "U.S. Accelerating Cyber Weapon Research," **Washington Post**, 18 March 2012. See, Andrey Nikishin, ICS Threats: A

Kaspersky Lab view, predictions and reality", http://campaigns.codenomicon.marketing/hubfs/CodenomiCON_Asia15_-_Andrey_Nikishin.pdf?t=1438746812613, (Accessed on 03.08.2015)

economy and innovation.⁴²⁶ Computer networks have no geographical borders that need to be crossed for an attacker to steal information. This grants freedom to any attacker to pick his target anywhere in the world and carry out a cyber attack. Therefore, securing computer systems is as important as securing physical entities from being attacked.



Source:

<http://www.heritage.org/static/reportimages/8F499ABD2700E7894534424D9F67D07B.jpg>

⁴²⁶ To emphasize how vulnerable nuclear facilities are to attack, the report also gave several accounts of 'known cyber security incidents at nuclear facilities' between 1992 and 2014: At **Ignalina nuclear power plant (1992)** in Lithuania, a technician intentionally introduced a virus into the industrial control system, which he claimed was "to highlight cyber security vulnerabilities". The **David-Besse nuclear power plant (2003)** in Ohio was infected by the Slammer worm which disabled a safety monitoring system for almost five hours. The **Browns Ferry nuclear power plant (2006)** in Alabama experienced a malfunction of both the reactor recirculation pumps and the condensate demineralize controller (a type of PLC). The **Hatch nuclear power plant (2008)** was shut down as an unintended consequence of a contractor's software update. An **Unnamed Russian nuclear power plant (circa 2010)** was revealed by Eugene Kaspersky to have been "badly infected by Stuxnet". South Korea's **Korea Hydro and Nuclear Power Co. commercial network (2014)** was breached, and information was stolen. The attack was subsequently attributed to North Korea, **Natanz Nuclear Facility and Bushehr Nuclear Power Plant (2010)**. Harriet Stanford: "Cyber Security: The Power Plant Problem", M 247, 5 October 2015, <http://m247.com/blog/cybersecurity-the-power-plant-problem/>

Recent high-profile cyber attacks, including the deployment of the sophisticated 2010 Stuxnet worm, have raised new concerns about the cyber security vulnerabilities of nuclear facilities. As cyber criminals, states and terrorist groups increase their online activities, the fear of a serious cyber attack is ever present. This is of particular concern because of the risk –even if remote– of a release of ionizing radiation as a result of such an attack. Moreover, even a small-scale cyber security incident at a nuclear facility would be likely to have a disproportionate effect on public opinion and the future of the civil nuclear industry.⁴²⁷ At the same time, the threats are getting more complex; the attackers are becoming more persistent. Protection of critical networks against cyber warfare requires detection of unknown threats. In the past, espionage was expensive, difficult, and extremely risky for the individuals and potentially the countries involved. The advent of the Internet changed all that by dramatically lowering the bar for entry into the world of espionage. Geographic distance, cultural adaption and threat of capture, have all disappeared in cyber space. This change also creates a low barrier against organized criminals and terrorists, which can also use online capabilities to steal or destroy.⁴²⁸

Yukiya Amano, Director General of the International Atomic Energy Agency (IAEA), said plainly, “Terrorists and other criminals operate international networks and could strike anywhere”. Pointing out that reports of actual or attempted cyber attacks are virtually a daily occurrence, Amano told attendees the nuclear industry has not been immune. “Last year alone, there were cases of random malware-based attacks at nuclear power plants, and of such facilities being specifically targeted,” he reported.⁴²⁹ Nuclear facilities have remained at the top of the global security agenda and have been a source of continuing conflict. The international community came to a close, a new kind of warfare has begun to eclipse international concerns that cyber terrorism threat has begun to overtake the traditional concerns about weapons of mass destruction and their proliferation. Therefore, the following institutional measures would strengthen⁴³⁰ nuclear safety and security:

⁴²⁷ Caroline Baylon, Roger Brunt, David Livingstone: “Cyber Security at Civil Nuclear Facilities-Understanding the Risks”, *Chatham House*, September 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

⁴²⁸ Bryce Boland, “Networks on Fire: Defending Critical Government Networks”, Cyber security Some Critical Insights and Perspectives” in **Cyber Security Some Critical Insights and Perspectives**, edited by Damien D. Cheong, Nanyang Technological University S. Rajaraha School of International Studies, pp.13-21.

⁴²⁹ “International response needed for cyber security threats to nuclear facilities”, 2 July 2015, <http://www.canadianunderwriter.ca/news/international-response-needed-for-cybersecurity-threats-to-nuclear-facilities/1003654812/?er=NA>, (Accessed on 05.08.2015).

⁴³⁰ **High-level meetings** on safety-security should convene regularly to ensure that the interface receives adequate attention. The Nuclear Security Summits and the IAEA are effective venues for such senior-level discussions. Safety-security measures must be built into a plant in **all its phases, from design and construction to routine operation** to decommissioning and dismantlement. Safety and security thus begins at the drawing board,

- Raise awareness of the nuclear safety-security intersection,
- Integrate the safety-security interface into nuclear facilities' service life,
- Establish post-Fukushima international standards for design basis accidents and design-basis threats, and
- Strengthen the IAEA's role to further assist national regulators.

Cyber risks are managed through evaluation of threats and vulnerabilities to computer and control systems during the life cycle phases as documented in the processes. Threats to the cyber security of critical infrastructures emanate from a wide spectrum of prospective perpetrators: state-sponsored espionage and sabotage, international terrorism, domestic militants, malevolent "hacktivists" or even disaffected insiders. Most of the efforts to reduce the risks of nuclear terrorism focus on preventing external attacks that could create a Chernobyl-like event or would enable a terrorist to steal fissile material to make a nuclear bomb. The risk of nuclear terrorism is changing and growing more complex in an era of cyber attacks and increasing competition between the United States and rising powers.⁴³¹ Cyber terrorism is an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. The threat posed by cyber terrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry.⁴³² The energy sector is under almost constant cyber attack

with an assessment of candidate sites for the plant and the design of the installation itself. This integration includes considerations of cyber intrusion and aircraft attacks that cannot be guarded against by traditional security methods. The primary cause of the station blackout at Fukushima was a beyond-design-basis accident. As currently calculated, **design-basis threats also might fail to cover the spectrum** of possible terrorist attacks. It is important to establish post-Fukushima international standards for both design-basis accidents and threats. These standards would consider an expansive list of possible accidents and incidents whether caused by internal events like malfunctioning safety systems and human error or external events like earthquakes, fires, floods, tornadoes, and terrorist attacks. To establish such international standards for design-basis accidents and threats that do not infringe on sovereignty and confidentiality, the IAEA should create model documents that respective countries can adapt to the specifics of their nuclear plants. National regulators have primary responsibility and authority for nuclear safety-security, but the **IAEA should continue being the main agency** to provide advice and expertise that help strengthen the safety-security interface around the world. In particular, the IAEA should encourage countries to accept the International Physical Protection Advisory Service, as well as the International State System of Accountancy and Control Advisory Service missions. These missions review practices across countries and at individual nuclear plants explaining how safety and security regimes compare with international guidelines and best practices, recommending improvements, and providing follow-up assistance. The highest levels of leadership and management in each country are also needed to ensure an effective balance between safety and security. Duyeon Kim, Jungmin Kang, *ibid.*

⁴³¹ "The Risk of Nuclear Terrorism from Insider Threats", *Bulletin of the American Academy of Arts & Sciences*, Projects and Activities, Summer 2014, https://www.amacad.org/multimedia/pdfs/publications/bulletin/summer2014/bulletin_Summer2014_InsiderThreats.pdf, (Accessed on 05.08.2015).

⁴³² Journalists, politicians, and experts in a variety of fields have popularized a scenario in which sophisticated cyber terrorists electronically break into computers that control dams or

while some attacks focus specifically on nuclear. In 2015, terrorist organizations and organized crime members can easily the set-up of the internet which is extremely friendly as well as they can harm the credibility of media that have become the main communications system. The most promising early areas for international cyber cooperation are probably not bilateral conflicts but problems posed by third parties such as criminals and terrorists. It is likely that major governments will eventually give higher priority to cooperation that works against the insecurity created by non-state actors with cyber weaponry. But the world is far from such a response at this stage of cyber development, just as the major powers did not begin such cooperation on nuclear weapons until the third decade of the nuclear era.⁴³³

- Can terrorist assaults target nuclear plants?
- Could terrorists cripple critical military, financial, and service computer systems?
- Who are the attackers?

As noted earlier in the introduction, today, radical terrorists of various kinds – anarchists, nationalists, separatists, revolutionaries, neo-Marxists, and fascists – are using the network to distribute their propaganda, to communicate with supporters, to create followers, and to overall execute their operations. Cyber terrorist attacks would aim to target the nuclear power plant off the line by interrupting the IT network power to the switch yard at the plants and create a big chaos and panic environment. Cyber attacks carried out by the citizens of a state against targets within that state may violate the laws of the state, and this may be identified as acts of domestic terrorism. Until now, no cyber attacks on nuclear power plants have resulted in releases of radioactive material, but the trends are profound.⁴³⁴ *Given the potential for great harm, any successful cyber attack on a nuclear facility would—at the least—undermine confidence in the ability of the state to be a responsible host and the owner and operator to run the facility in a safe and secure manner.* Cyber attacks may be intended to have local and limited effects, but radioactive material ejected from a failed reactor pays no heed to national boundaries. Foreign governments, groups hostile to the government of a given state, or individuals motivated by greed, hatred or curiosity may carry out cyber

air traffic control systems, wreaking havoc and endangering not only millions of lives but national security itself. And yet, despite all the gloomy predictions of a cyber generated doomsday, no single instance of real cyber terrorism has been recorded. Gabriel Weimann, “Cyber Terrorism: The Sum of All Fears?”, *Studies in Conflict & Terrorism*, Vol. 28, Issue 2, 2005, pp. 129–149.

⁴³³ Joseph S. Nye, Jr., “From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?”, *Bulletin of the Atomic Scientists*, 2013, Vol. 69, No. 5, pp. 8–14.

⁴³⁴ Cyber Security Strictly Regulated by NRC, “No Additional Regulation Needed”, *Nuclear Energy Institute Policy Brief*, March 2014,

<http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy-Briefs/CyberSecurity-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf>, (Accessed on 07.08.2015).

attacks. The systems intended to deter and defeat such threats must address all potential perpetrators, taking into consideration the range of motivations noted above:

- a. Cyber attacks carried out by the citizens of a state against targets within that state may violate the laws of the state intended to protect the public health and welfare and may be identified as acts of domestic terrorism,
- b. Cyber attacks created by activities outside the targeted state or affecting other states in addition to the targeted state may be considered as acts of international terrorism,
- c. Cyber attacks carried out by or under the aegis of foreign governments may be considered as acts of war, and
- d. Cyber attacks in certain circumstances might be classified as crimes against humanity.

Contemporary nuclear power plants rely extensively on a large and diverse array of computers for a host of tasks. Some computers may play a role in monitoring or controlling the operation of the reactor itself or of ancillary systems. The nuclear power plant operating and technical support staff commonly uses computer networks, and connections may exist between these systems and plant control systems, sometimes known, sometimes unknown. If the hardware or software used is modified or replaced, the reactor might be forced into an accident and the emergency response systems may fail to prevent calamity.⁴³⁵

Today's cyber attacks are made on computer systems operated for a wide spectrum of purposes. The IAEA has identified four significant risk scenarios involving cyber attacks on civil nuclear facilities:

- **A cyber attack** that corrupts a civil nuclear facility's command and control system, leading to the unauthorized removal of nuclear or another radioactive material. Such an attack would most likely be carried out by a terrorist organization, or by a criminal organization wanting to blackmail a state or company.
- **An act of cyber sabotage** which affects the normal functioning of a nuclear facility or other parts of the nuclear fuel cycle. States, terrorist organizations, political activists (for example, environmentalist groups) and criminals may all have an interest in this type of furtive cyber operation.
- **An act of cyber espionage** which results in the collection and exploitation of sensitive nuclear information. This information might be used by a terrorist

⁴³⁵ Maurizio Martellini, "Cyber Security for Nuclear Power Plants", US State of Department, Washington, DC, January 2012, <http://www.state.gov/t/isn/183589.htm>

organization, criminal or state willing to acquire, smuggle or use nuclear material or information for malicious purposes.

- **Theft** of nuclear sensitive information⁴³⁶

In fact, cyber attacks resulting in physical damage can cause various symptoms in the field, including rising temperature, strange sounds, and abnormal vibration. The owners of a nuclear power plant based in South Korea have announced that they will conduct a series of tests to evaluate how well its networks can withstand an attack. Korea Hydro and Nuclear Power Co (KHNP) made the decision after hackers leaked the designs and manuals of plant equipment online. The hackers also threatened an attack against the plant if it did not cease operations by Christmas Day.⁴³⁷ Small commercial drones for express parcel delivery to military ones were used to attack terrorist suspects. Yet the prospect of increasing numbers of drones filling the skies poses abundant security concerns for critical infrastructure –including for the nuclear industry.⁴³⁸ Drones, or unmanned aerial vehicles, have been in the news lately. Last fall, unidentified drones breached restricted airspace over 13 of France's 19 nuclear power plants in a seemingly coordinated fashion. In January, a drone crashed onto the lawn of the White House. Recently, a drone was found on the roof of the Japanese Prime Minister's office. There are ways to detect and intercept drones, such as jamming radio signals or using helicopters to pursue encroaching drones. Chinese scientists are developing a laser weapon that can detect and shoot down small, low-flying aircraft, and interception drones have the ability to drop nets over intruding drones. However, there are many legal issues that challenge the use of these techniques.⁴³⁹ Cyber security is also regarded as one of the most critical issues for the Euro-Atlantic Community's leading military organization namely North Atlantic Treaty

⁴³⁶ <http://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-21-05-24-TM-NPTD/day- 1/5.cybersecurity-dudenhoeffer.pdf>

⁴³⁷ David Bisson, "Korean Nuclear Power Plant Plans Cyber Attack Drills In Wake of Hacker Threats", *Tripwire*, 22 December 2014, <http://www.tripwire.com/state-of-security/featured/korean-nuclear-power-plant-plans-cyberattack-drills-in-wake-of-hacker-threats/>, (Accessed on 07.08.2015).

⁴³⁸ The flights over French facilities have exposed nuclear plants' lack of adequate defenses against drones. This has left the French government—while outwardly reassuring the public that it has put in place 'all means necessary to protect nuclear installations'—scrambling to find adequate solutions. Caroline Baylon, "Drones: The Threat to Nuclear Plants", *Newsweek*, 27 December 2014, <http://www.newsweek.com/drones-threat-nuclear-plants-294458>, (Accessed on 07.08.2015).

⁴³⁹ The Federal Aviation Administration (FAA) has a long-standing "Notice to Airmen" warning pilots not to linger over nuclear power plants. The FAA has also issued guidelines on where users should not fly drones, but the industry is largely unregulated as more companies look to use the relatively new technology in their businesses. The FAA has been working to craft a comprehensive regulatory framework for drones, following calls from Congress and the President, and recently issued draft regulations for the commercial use of drones. Monika Coflin, "Droning on over Nuclear Power Plants", *United States Nuclear Regulatory Commission*, 23 April 2015, <http://public-blog.nrc-gateway.gov/2015/04/23/droning-on-over-nuclear-power-plants/>, (Accessed on 10.08.2015).

Organization (NATO). For the last couple of years, one of the most widely discussed issues in NATO's summits has been the cyber threats which can seriously damage the functioning of all systems in the Allied countries. For instance, in the 2014 NATO Wales Summit Final Declaration⁴⁴⁰ there exist two paragraphs with regard to this issue. They are as follows;

"Paragraph 72 - As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defense Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defense. It recalls that the fundamental cyber defense responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyber space. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defense is part of NATO's core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.

Paragraph 73 - We are committed to developing further our national cyber defense capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defense capabilities of the Alliance. We will continue to integrate cyber defense into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organizations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defense Policy's objectives. We will improve the level of NATO's cyber defense education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the

⁴⁴⁰ For a detailed analysis on the NATO 2014 Wales Summit please see, Mesut Hakkı Caşın, "The Future of NATO and Atlantic Security after the 2014 Wales Summit", in **Geopolitics of the Caspian Region**, ed. Ahmet Yükleyen, (İstanbul: Caspian Strategy Institute, 2015), pp. 107-120.

*capabilities and requirements of the NATO CIS School and other NATO training and education bodies.*⁴⁴¹

Cyber Security Mechanism for Nuclear Energy Plants

Cyber security refers to the prevention, detection, and mitigation of unauthorized attempts to control or disable computers and electronic control systems as well as to the protection of information in computer databases. Cyber security is commonly understood to have three attributes: confidentiality, availability, and integrity. Security risks cannot be reduced to zero. Managing ICS requires a systematic, comprehensive, and dynamic methodology. Every day new viruses, new vulnerabilities, and new problems are found with the systems.⁴⁴² Cyber space is a new and evolving realm of human interaction with specific security and defense concerns. Threats to commercial and government interests are being identified and many nations have accepted cyber space as a domain of military operations. The relation between cyber space and national security is often non-separated issues for modern states. But states' cyber capabilities are already widely dispersed and are not the monopoly of a few countries. Recent high-profile cyber attacks on nuclear facilities have raised new concerns about the vulnerability of nuclear power plants. Cyber criminal groups are becoming increasingly skilled. Organized criminal groups might steal confidential information belonging to a nuclear facility and then blackmail the facility into paying a ransom to prevent it from being released.

For example, Stuxnet, unlike the malware that came before it, is highly targeted and designed to achieve a real-world outcome. Stuxnet has challenged assumptions about nuclear facilities which are claiming that the facilities are not connected to the Internet and the belief that network defenses will protect facilities from vulnerabilities in software applications. Whatever the cost to create Stuxnet, it was far less than the cost of a traditional military attack. Future versions of Stuxnet may be used by nation states, terrorist groups, hacktivists and cyber criminals to achieve their own goals. In the future, cyber weapons may not be as restrained as Stuxnet. This malware has started a new arms race, and has created serious implications for the security of critical infrastructure worldwide. In September 2010, the Bushehr nuclear power plant was believed to be infected by Stuxnet. The Stuxnet worm heralded the advent of a new era in cyber warfare. The attacks caused the partial destruction of around 1,000 centrifuges. This was the most highly sophisticated publicly known cyber attack on a nuclear facility to date, demonstrating an unprecedented level of technical capabilities.

⁴⁴¹ North Atlantic Treaty Organization, "Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales 05 September 2014, Press Release (2014) 120 Issued on 5 September 2014, Last updated: 31 July 2015, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Accessed on 24.08.2015).

⁴⁴²"Cybersecurity at Civilian Nuclear Facilities", http://www.nap.edu/openbook.php?record_id=18412&page=72, (Accessed on 10.08.2015).

This speculation came about from the delayed start-up of the Russian-built facility. Ali Akbar Salehi, the head of the Iranian Atomic Energy Organization, stated that the plant was no longer being “affected” by Stuxnet and the delay was due to “hot weather”. Stuxnet demonstrated that the attackers knew more about the hardware and software than the system owners.⁴⁴³ According to Gen. Michael V. Hayden, former director of the Central Intelligence Agency (CIA) and the National Security Agency (NSA), Stuxnet is “the first attack of a major nature in which a cyber attack was used to effect physical destruction”.⁴⁴⁴ Another critical accident was faced in South Korea’s state-run nuclear operator which was the subject of a cyber attack in 2014. The cyber attackers aimed to illegally get information about the nuclear reactors and electrical flow systems. President Park Geun-hye ordered a complete inspection of South Korea’s key national infrastructure against what she called “cyber terrorism”. “Nuclear power plants are first-class security installations that directly impact the safety of the people,” Park said.⁴⁴⁵

As we noted earlier, the cyber domain, a cyber security impact analysis is performed before making changes to the relevant equipment. The effectiveness of cyber security controls is periodically assessed, and enhancements are made where necessary. Vulnerability assessments are performed to ensure that the cyber security posture of the equipment is maintained. Cyber security for a nuclear facility can be divided into two parts: instrument and control security (ICS), and facility network security (FNS). There are several differences between these parts of security, including different methodologies, mechanisms, and the effect of failure in each domain. Cyber security in a nuclear power plant cannot be accomplished by a single person, a single team, or a single company. Computer systems that help operate nuclear power plants and safety equipment is isolated from the Internet and from internal computer networks to protect against outside intrusion. Strict controls govern the use of portable media, such as thumb drives, CDs, and portable computers. In addition, nuclear plants are designed to automatically disconnect from the power grid if there is a disturbance that could be

⁴⁴³ For the first time a computer worm, through malicious manipulation, caused physical destruction in the real world. The Stuxnet worm was a malware program so complex that it could stealthily move from system to system, replicating itself and effectively reprogram critical systems while hiding the modified code from human controllers. Stuxnet only performed repairable damage to the Iranian nuclear facilities, most likely because it was programmed to do so. This was, however, the intention of the writers of Stuxnet rather than a limitation of the technology; such restraint may well not be the aim of future malware. Sean Collins, Stephen McCombie, “Stuxnet: The Emergence of a New Cyber Weapon and Its Implications”, *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, April 2012, pp. 80-91.

⁴⁴⁴ Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare”, *Security Studies*, 2013, Vol. 22, pp. 365–404.

⁴⁴⁵ “South Korean Nuclear Operator Hacked Amid Cyber Attack Fears”, *The Guardian*, 22 December 2014, <http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyberattack-hack>.

caused by a cyber attack.⁴⁴⁶ When these computer systems are attacked or hacked by malicious elements, at a minimum certain functionalities of the plant are affected to some extent, and such attacks can lead to serious accident conditions. Cyber security refers to how to tackle such problems and how to protect computer bases against malicious attacks by external elements.

As cyber security no longer remains just a matter of corporate choice, its budgets are escalating. Forecasts indicate that the global cyber security market will increase from \$80 billion at present to over \$140 billion by 2017.⁴⁴⁷ The objective of a cyber attack may not be to cause death and destruction, for example, but to disrupt the operation of a nuclear facility, to inflict economic damage, to embarrass government or utility officials, to blackmail companies, to get even, or just to test one's skills or to see what happens.⁴⁴⁸

In order to keep safe, all power reactor licensees must implement a cyber security plan and regulation. Cyber security experts have recently emphasized the need to integrate the management of cyber risks into enterprise risk management. Their point certainly applies to risk management at nuclear facilities, such as reactors and storage, where digital controls are vulnerable to operating failures and attacks.⁴⁴⁹ Critical safety, security and emergency preparedness systems at nuclear energy facilities are isolated from the Internet. In addition, nuclear power plants are designed to shut down safely should their systems detect a disturbance on the electrical grid. Thus, nuclear plants are protected from digital threats by layer upon layer of safety measures.⁴⁵⁰ Each nuclear power plant's cyber security program protects its digital computer and communication systems and networks against cyber attacks, including systems and networks associated with:

- Safety-related functions and secondary functions considered “important-to-safety”,
- Security functions,
- Emergency preparedness functions, including offsite communications, and

⁴⁴⁶ “Nuclear Power Plant Security”, *Nuclear Energy Institute-NEI Fact Sheets*, September 2014, <http://www.nei.org/master-document-folder/backgrounders/fact-sheets/nuclear-power-plant-security>, (Accessed on 10.08.2015).

⁴⁴⁷ Suryakanthi Tripathi, “Cyber: Also a Domain of War and Terror”, *Strategic Analysis*, Vol. 39, No.1, 2015, pp.1-8.

⁴⁴⁸ U.S. Department of State 01/23/12 Paper - Cyber Security for Nuclear Power Plants, “Cyber Security for Nuclear Power Plants Prepared by Maurizio Martellini, Thomas Shea, and Sandro Gaycken”, January 2012, <http://www.state.gov/t/isn/183589.htm>, (Accessed on 10.08.2015).

⁴⁴⁹ Chris Spirito, Hurwitz, R., Shrobe, H, “Integrating Cyber Dimensions in Recognizing and Responding to Threats to Nuclear Facilities: Challenges and Lessons of Recent High Profile Cyber Incidents”, *IAEA Conference*, IAEA-CN-228/5B2/140.

⁴⁵⁰ <http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/CyberSecurity-Strictly-Regulated-by-NRC;-No-Addit>

- Support systems and equipment important to safety and security.⁴⁵¹

Human Factor in Nuclear Plant Security and Role of the Training

Today and in the future, advanced information technology has been more reliable, so human failure becomes the prevalent cause of nuclear incidents. Notably, human and organizational factors have always had a major influence on the safety of high-risk process industries. In particular, in the case of the nuclear industry, they intervene in all phases of the lifecycle.⁴⁵² The existence and implementation of operating procedures in hazardous industries, as the nuclear power industry, should support a high level of safety for the plants. Humans are integral to the safe operation of a nuclear power plant. Defensive cyber operators are similar to 24-hour occupations that have been well studied in the human factors community, such as nuclear plant operators; however they are unique in several key respects. However, the nuclear energy industry maintains very strict security to prevent unauthorized persons from gaining access to critical equipment. Malicious individuals and groups, whether aiming to steal personal information or to completely destabilize an Internet network or critical infrastructure system, can expose sensitive personal and business information and disrupt critical operations. Human factors research and practice should seek to help manage workload within cyber operations teams, cope with shift work, enhance relevance and effectiveness of training, and minimize the impacts of organizational change. We see the importance of human performance is also an effect of the significant improvement of nuclear technology.⁴⁵³

⁴⁵¹ United States Nuclear Regulatory Commission, “Backgrounder on Cyber Security”, December 2014, <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html>, (Accessed on 12.08.2015).

⁴⁵² In a complex industrial facility such as a nuclear power plant, the majority of the tasks are performed by machines. But man is, of course, involved to a great extent in their design, testing, maintenance and operation. The performance of a person working within a complex mechanical system depends on that person's capabilities, limitations and attitudes, as well as on the quality of instructions and training provided. The interface between a machine and its operators in any industrial project is usually known as the human factor. OECD-Nuclear Energy Agency, “The human factor in nuclear power plant operation”, No. 2, January 1988, <https://www.oecd-nea.org/brief/brief-02.html>, (Accessed on 13.08.2015).

⁴⁵³ There are also significant issues in the culture of the industry that contribute to the challenge. The different priorities and ways of thinking of nuclear plant personnel, who are operational technology (OT) engineers, and cyber security personnel, who are information technology (IT) engineers, frequently lead to misunderstandings. The problem is exacerbated by the fact that cyber security personnel are often located at a considerable distance from nuclear facilities and rarely visit. Furthermore, the level and quality of cyber security training at nuclear facilities are insufficient: in addition to a lack of cyber drills, nuclear personnel may have a poor understanding of key procedures, in part as a consequence of the cultural divide, since the training material is written by IT engineers. Thus nuclear plants may lack preparedness for a large-scale cyber security emergency, particularly one that occurs after normal working hours.

Regardless of the type of threat, the sources of threats are either internal or external to the company. A company's internal agent threat is "...an employee of the company that has greater access to sensitive information, a better understanding of internal processes, and knowledge of high-value targets and potential weaknesses in security". Internal agent attacks are also called internal penetration or insider attacks. The literature identifies that internal agent attacks "...are more frequent than external attacks", and involve, among other types of attacks "making an unintentional mistake"; and, in general, do not account for much of the company losses due to cyber crimes. Also, "by most accounts... unintentional human actions (or omissions) cause a large fraction of system incidents that are not explained by natural events and accidents. These sources identify that internal agent threats of an unintentional nature are more frequent, i.e. high, yet do not result in a major financial impact to the organization. For external agent attacks, unintended mistakes, similar to that of internal agent attacks, are considered extremely unlikely. These attack scenarios and processes are different, so the probability that an external agent would make an unintended mistake, as previously defined, was rated low. Moving from unintended mistakes to threats associated with purposeful intent, there are two questions of interest. First, what are the key motivators? Second, are internal and external threat motivators different? The literature identifies that intentional internal agent attacks "...least frequently occur", and are often motivated by financial gain or malicious intent. Specifically, in an insider threat study or an analysis of validated cases of insider attacks indicated that "...motivation was financial gain". Another example is the often-cited Australian 2011 waste water attack, that was initiated by an "...ex-employee [who] was trying to convince the water treatment company to hire him to solve the problems he was creating". Thus, for intentional insider attacks, financial gain is identified as a key motivator, but the frequency of occurrence is lower than unintentional insider attacks, so a probability of moderate was assigned. Further, external agent threat motivation may be the desire to obtain system command and control capability, providing remote data access, data exfiltration, data manipulation, or activity monitoring.⁴⁵⁴

Nuclear facilities that allow third-party remote access may open up several new avenues by which hackers can gain access. The owner-operators' commercial network can serve as a route of infection. Owner-operators are increasingly creating direct links between their corporate business networks and facilities' industrial control system networks. In many cases, the plants will employ optical data diodes, which allow unidirectional communication (i.e. allow data to flow outwards but not inwards) by beaming a laser through a fiber optic cable from inside the plant to an external receiver. The receiver detects the light and converts it into data form; it has no ability to transmit data back, making the system nearly impossible to breach (except perhaps by a highly advanced state actor). In other instances, however, these links may not be adequately

⁴⁵⁴ Morgan Henrie, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment", *Engineering Management Journal*, 2015, Vol.25, No.2, pp.38-45.

protected and a hacker may be able to use the corporate business network to gain access to the nuclear facility's industrial control systems.

The cyber security threat requires an organizational response by the civil nuclear sector, which includes, by necessity, knowledgeable leadership at the highest levels, and dynamic contributions by management, staff and the wider community of stakeholders, including members of the security and safety communities. Some recommendations could be summarized as follows:

Develop guidelines to measure cyber security risk in the nuclear industry, including an integrated risk assessment that takes both security and safety measures into account. This will help improve understanding of the risk among CEOs and company boards and make cyber security in the nuclear sector more commercially attractive.

Promote cyber insurance, which will require strong risk assessments, as an effective way to drive the process of implementing change.

Engage in robust dialogue with engineers and contractors to raise awareness of the cyber security risk, including the dangers of setting up unauthorized internet connections.

Establish rules where these are not already in place –such as banning personal devices from control rooms and requiring nuclear plant personnel to change the default passwords on equipment– and enforce these rules through a combination of independent verification methods and technical measures, for example by blocking off USB ports.

Encourage nuclear facilities to share threat information anonymously (such as by revealing 'indicators of compromise') in order to promote greater disclosure, since the reluctance to disclose cyber attacks stems partly from concerns for damage to reputation.

Promote industry conferences and other measures to enhance interpersonal relationships in order to encourage informal sharing initiatives, even if governments are dissuaded by national security concerns from sharing threat information at the international level.

Governments should lead the establishment of national Computer Emergency Response Teams (CERTs) specialized in industrial control systems, particularly since they recognize that information sharing at a national level is key.

The regulator should reassure owner-operators that they will not be penalized for any information they share, provided they show good faith.

Encourage all countries that have not yet done so to adopt an effective regulatory approach to cyber security at nuclear facilities. Since a large number of countries follow IAEA guidance, allocating more resources to the IAEA to enable it to develop recommendations on responding to cyber security threats could generate significant benefit.

Provide technical and funding assistance to developing countries in order to improve cyber security at their nuclear facilities.

Establish integrated projects between nuclear plant personnel and cyber security personnel, such as the preparation of cyber security training materials and undertaking of joint vulnerability analyzes. This would also encourage IT personnel to visit the nuclear facility in person on a regular basis to aid mutual understanding.

Improve the frequency and quality of cyber security training at nuclear facilities, potentially involving accreditation of training programs by the IAEA, and hold integrated scenario-led drills between nuclear plant personnel and cyber security personnel to hone skills and develop common understandings and practices.

Promote the further creation of more cross-disciplinary university programs aimed at training cyber security specialists in the nuclear industry.

Foster partnerships between vendors and cyber security companies to enable the development of more robust cyber security products.⁴⁵⁵

As we summarized above, there is already a very long history of human factors in the nuclear power industry albeit with a predominant focus on safety. In fact, notwithstanding recent high-profile events, nuclear power is probably the safest high-hazard industry and most certainly far safer than healthcare.⁴⁵⁶ From a security perspective, human performance errors are one of the most common causes for issues and events in nuclear energy plants. On the other hand, there has been limited work examining cyber attacks from a human-centered perspective. Humans play a role in all aspects of nuclear plants security, including the functions of deterrence, detection, and response and in the capacities of both administrators and recipients of security procedures. The field of human factors has contributed to critical infrastructures security functions. These obligations need to design of user-centered technology and training programs, through metrics for assessing human performance, through environmental design, and through organizational changes targeting the larger socio-technical system. Greater attention is being paid to human needs in designing

⁴⁵⁵ Caroline Baylon, Roger Brunt, David Livingstone, *ibid*, p.21.

⁴⁵⁶ Chris Lo, "Nuclear plant operations: Unlocking the Human Factor", 26 February 2015, <http://www.power-technology.com/features/feature-nuclear-plant-operations-unlocking-the-human-factor-4516904/>, (Accessed on 13.08.2015).

equipment, and efforts are being made to learn from experiences in order to correct past errors. In this regard, we aim to review these and other contributions for future research and development on human factors for nuclear facilities security issues. We indicate that the field of human factors provides many low-cost, high-impact solutions that reach beyond the bounds of the human–single machine interface. For example, “the command and control networks used to control nuclear weapons might be targets of cyber attack.” We think a current lack of knowledge regarding the effects of cyber attacks on human behavior and performance represents a critical knowledge gap.

Since the beginning of the nuclear power generation, human performance has been a very important factor in all phases of the plant lifecycle: design, commissioning, operation, maintenance, surveillance, modification, decommissioning and dismantling. This aspect has been confirmed by recent operating experience. In fact, 48% of the events reported in the IAEA/NEA Incident Reporting System (IRS) are affected by human errors. Moreover, about 63% of the events reported in IRS and having significant human contribution happened during operation and 37% during shut-down. The optimization of nuclear plants security policies requires a large effort of development of new techniques and models, particularly methods and risk-informed techniques, and improved awareness and insight of human factors, organizational design and culture.⁴⁵⁷ In order to develop guidance to enlarge the capacity of the nuclear safety culture in the context of human factors, we need to improve the synergy between technology and human and organizational factors. However, considering nuclear events in the real picture, experts insist on to us we must acknowledge that nuclear facilities can never be 'absolutely safe', so we must prepare to manage unexpected events.⁴⁵⁸ Physical and electronic barriers do a significant and effective job of denying those with malicious intent to do harm to our nuclear stations, but unless employees consistently perform as they should, damage to plant systems can be substantial.⁴⁵⁹ In this regard, we need education and culture in nuclear security in general and in computer security in particular, which will play an important role in ensuring that the next generation of leaders are well educated and are able to take the appropriate measures to protect those computer systems, networks, and other digital systems from malevolent acts.

⁴⁵⁷ Giustino Manna, “Human and Organizational Factors in Nuclear Installations: Analysis of available models and identification of R&D issues”, European Commission Joint Research Centre Institute for Energy – Scientific and Technical Reports, 2007, <http://iet.jrc.ec.europa.eu/senuf/sites/safelife.jrc.ec.europa.eu.senuf/files/files/documents/eur-23226.pdf>, (Accessed on 14.08.2015).

⁴⁵⁸ Greg Webb, “Experts Conclude Meeting to Discuss "Human Factors" of Nuclear Safety”, 27 May 2013, <https://www.iaea.org/newscenter/news/experts-conclude-meeting-discuss-human-factors-nuclear-safety>, (Accessed on 14.08.2015).

⁴⁵⁹ Jane LeClair, K. Newmeyer, “Social Engineering: A Threat to the Nuclear Industry”, IAEA Conference, 2015.

Legal Framework of Nuclear Facilities Security

Nuclear and associated facilities and systems are not immune to cyber threats. Cyber war and economic espionage are largely associated with states; cyber crime and cyber terrorism are mostly associated with non-state actors. At present, the highest costs come from espionage and crime, but over the next decade or so, sabotage, war, and terrorism may become greater threats than they are today. The problem of protection of critical infrastructure against cyber criminality now requires greater attention both from the side of the international community and various states and institutions. Naturally, the question of legal provision for protection against cyber criminality and studies of the methods of protection of sensitive information from the actions of cyber criminals become the issues of the highest priority for corresponding specialists.⁴⁶⁰ The question of what international and legal frameworks apply in case of a cyber attack against a nuclear facility depends on several factors. First, it depends on the intent and the effects of the cyber attack. Was it to acquire information (cyber espionage) or was it to disturb the normal functioning of the nuclear facility (cyber sabotage)?⁴⁶¹ Art of answering this question requires a perspective from international that the legal question as old as crime and punishment: Who did it? Dealing with a phenomenon that may arise in the future but has hardly occurred so far in the practice of states and non-state actors, physical security at nuclear power plants involves the threat of radiological sabotage –a deliberate act against a plant that could directly or indirectly endanger public health and safety through exposure to radiation. Different from other targets, cyber attacks involving nuclear material and/or nuclear facilities, in a worst-case scenario, could pose the risk of radioactive release, which would compound resultant damage to human health, the environment, and economies. This means that although certain cyber threats are addressed by more general international legal frameworks.⁴⁶²

The only international agreement so far in the cyber domain has been the Budapest Convention on Cyber Crime⁴⁶³ which came into effect in 2004. Developed by the Council of Europe, the convention is yet to garner widespread ratification. The current international nuclear security framework consists of conventions such as the

⁴⁶⁰ Drapey, S, Gavryliuk, V, Gavryliuk-Burakova, A. Parkhomenko, V. Proskurin, D. Romanova, O., Samsonenko, A., "Implementation of Computer Security Culture in the Scope of Physical Protection in Ukraine", *IAEA Conference*, 2015.

⁴⁶¹ V. Boulanin, "International and Legal Frameworks Addressing Cyber Attacks against Nuclear Facilities: The State of Play".

⁴⁶² J. Herbach, "Developing the International Law Framework to Better Address Cyber Threats: Role of Non-Binding Instruments", Centre for Conflict and Security Law, University of Amsterdam,
http://conflictandsecuritylaw.org/web_documents/j_herbach_developing_the_international_law_framework_to_better_address_cyber_threats.pdf, (Accessed on 23.08.2015).

⁴⁶³ The Council of Europe, "Convention on Cyber Crime", Budapest, 23 November 2001,
<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, (Accessed on 23.08.2015).

Convention on the Physical Protection of Nuclear Material (CPPNM)⁴⁶⁴ and its 2005 Amendment⁴⁶⁵ and the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT).⁴⁶⁶ These treaties, however, are of limited application when it comes to addressing cyber threats, namely in regards to specific criminalization provisions. Sabotage under the CPPNM Amendment entails the intentional commission of acts against a nuclear facility, or acts interfering with the operation of nuclear facilities where the offender intentionally causes, or where the offender knows that the act is likely to cause death or harm to people, property or the environment.⁴⁶⁷ Legal scholars disagree over the applicability of the existing international norms, principles, and standards to cyber space activities. While some believe that the existing regulations and standards are not applicable to cyber space, there are those who believe that existing regulations are fully applicable to cyber space activities.⁴⁶⁸

From the international law perspective:

- a. The international community needs to review regularly whether the treaties and other measures in place are adequate. Such measures should reflect the fact that a cyber attack on a nuclear power plant with the intention of substantial radiation releases should be considered as act of terrorism and hence be prohibited by the International Convention for the Suppression of Acts of Nuclear Terrorism or a crime against humanity subject to other relevant anti-terrorism treaties, the Convention on the Physical Protection of Nuclear Material, or the Nuclear Safety Convention.
- b. It is incumbent on the national government of each state to establish an inter-departmental response to the threat of cyber attacks on nuclear power plants, including its national security structure in all of its dimensions. It may

⁴⁶⁴ U.S. Department of State Bureau of International Security and Nonproliferation, "Convention on the Physical Protection of Nuclear Material - Signed at New York March 3, 1980, Entered into force February 8, 1987", <http://www.state.gov/t/isn/5079.htm#treaty>, (Accessed on: 23.08. 2015).

⁴⁶⁵ International Atomic Energy Agency Board of Governors General Conference, "Nuclear Security – Measures to Protect Against Nuclear Terrorism Amendment to the Convention on the Physical Protection of Nuclear Material - GOV/INF/2005/10-GC(49)/INF/6 Date: 6 September 2005", <https://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf>, (Accessed on 23.08. 2015).

⁴⁶⁶ United Nations, "International Convention for the Suppression of Acts of Nuclear Terrorism -2005", <http://www.un.org/en/sc/ctc/docs/conventions/Conv13.pdf>, (Accessed on 23.08 2015).

⁴⁶⁷ http://conflictandsecuritylaw.org/web_documents/j_herbach_developing_the_international_law_framework_to_better_address_cyber_threats.pdf

⁴⁶⁸ Metodi Hadji-Janev, "Evaluating the Applicability of the Existing Principles and Standards of International Law to Cyber", *IAEA Conference*, 2015.

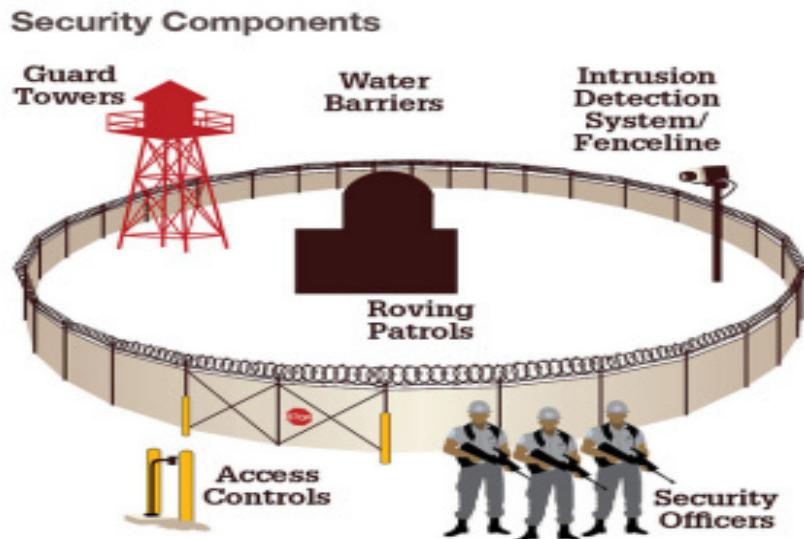
be appropriate to define such arrangements within an existing governmental body or to create a new agency for this and related purposes.

- c. It is further incumbent on each national government to enact legislation together with subordinate regulations and guidelines consistent with its legal structure and the threats it faces, in conformance with its treaty obligations and other considerations.

In the area of nuclear waste management, we know that each reactor produces 20 tons of nuclear waste per year, and this waste is locally stored, usually in steel casks at temporary waste sites. These casks can be penetrated by regular weapons and release radioactive cesium gas. Drones can be remotely controlled by a human pilot or programmed to follow pre-specified routes. Drones can travel into airborne radioactive plumes without exposing pilots and crew to radiation. But drones have a potential dark side. Reports of drones buzzing around French nuclear plants prompted considerable discussion about whether drones carrying explosives could wreak damage. The short answer is yes. Drones broadcasting loud sounds of explosions and gunfire, for example, could confuse and slow down the responders. Likewise, collisions with the perimeter fence –activating the intrusion-detection system– could send responders on time-consuming wild drone chases. Clearly, drones are double-edged swords: They can perform critical functions to protect the public in the event of a nuclear plant accident, but they can also perform tasks that could cause a nuclear plant disaster. How can authorities permit good drones while prohibiting bad ones?

Depending on the circumstances of individual attacks, the site security force, local law enforcement, national law enforcement and international bodies, especially Interpol, should be prepared to respond and be engaged as soon as possible. Law enforcement agencies have to develop sufficient capacities in the field of IT-forensics, including the undeveloped field of IT-forensics of Industrial Control Systems (ICS).

- a. Each state should enact and enforce legislation to prevent cyber attacks on nuclear reactors and nuclear fuel cycle facilities, detect and apprehend perpetrators and punish individuals or organizations operating within the territory of a state responsible for or abetting such activities.
- b. States should examine the provisions of existing conventions (especially the Convention for the Suppression of Acts of Nuclear Terrorism and the Convention for the Physical Protection of Nuclear Material) with the intention of identifying interpretations and/or modifications as necessary to extend their provisions to include domestic and international nuclear cyber terrorism.



Source:

<https://nrcpublicblog.files.wordpress.com/2013/08/security.jpg?w=300&h=280>

Conclusion

Successful attribution requires a range of skills on all levels, careful management, time, leadership, stress-testing, prudent communication, and recognizing limitations and challenges. Security risks cannot be reduced to zero. Well trained and armed security officers; equipment and structures, including physical barriers, intrusion detection and surveillance systems; and access controls. Another layer of protection is in place for coordinating threat information and response. Well-organized and well-financed non-state groups, like the Islamic State, may employ new tactics, technologies, and capabilities to steal nuclear materials. Governments must therefore consistently evaluate evolving technologies and threats so that security systems designed to protect nuclear materials stay ahead of the capabilities of those who would seek to steal them. Second, governments and industry should make sure that security culture, like safety culture, becomes an integral part of every nuclear facility's operations. As General Eugene Habiger, a former commander-in-chief of the United States Strategic Command who was the US Department of Energy's "security czar" once put it: "Good security is comprised of 20% equipment and 80% people." Governments and industry should work together to nurture a strong culture of security. Each and every employee at a nuclear facility –from guards to scientists to senior staff– must view the security of nuclear materials as an essential part of their jobs. Third, governments must regularly review security systems at nuclear facilities. It is not sufficient for nuclear operators to say that the state of security in their facilities is "good enough". Effective oversight can

root out complacency.⁴⁶⁹ Perhaps the greatest cyber security issue facing the nuclear industry is that many in the sector do not fully understand the risk, and therefore a key first step is to develop guidelines to assess and measure this risk as accurately as possible. This will help CEOs and company boards to understand what is at stake, and also provide them with a clear economic rationale to invest in cyber security.⁴⁷⁰ We consider today and in the future, using nuclear energy will increase the capacity of energy sources in the world economy. In this article, we see that nuclear power security is an important international phenomenon. Of course, using and to have nuclear power some advantages for energy supply but it's also large, complex, both financial and human capital intensive, using high technology techniques, needs seriously advanced security and safety for producing electricity. Therefore, in our study we tried to emphasize nuclear safety and security for preventing states and human civilization environmental and human health importance. We also stressed how the states and the international community can ensure safety and security in the nuclear energy sector from an international law perspective. In this regard, considering terrorism and cyber attacks threats we also try to understanding possibilities of the accidents, hostile sabotages, insider threats and preventive measures.

⁴⁶⁹ Des Browne and Igor S. Ivanov, "From Nuclear Safety to Nuclear Security", *Project Syndicate*, <http://www.project-syndicate.org/commentary/nuclear-security-fukushima-by-des-browne-and-igor-ivanov-2015-03>, (Accessed on 24.08.2015).

⁴⁷⁰ The development of cyber insurance, with its strong reliance on risk metrics, may be an important tool for promoting the development of cyber risk guidelines. In tackling the challenges related to the 'human factor', it will also be important to raise awareness among both engineers and contractors of the risks involved in setting up unauthorized connections or plugging in personal USBs at nuclear facilities. Measures that promote disclosure and information-sharing can also play an important role in enhancing cyber security, as can regulatory standards and other policy measures, improved communication to bridge cultural divides and the implementation of technical solutions. The apparent lack of preparedness for a large-scale cyber security emergency, particularly one that occurs outside normal working hours, also suggests that scenario-based planning studies and exercises would lead to a better understanding of how a situation might unfold in a crisis – and to the development of effective response plans across the industry. Caroline Baylon, Roger Brunt, David Livingstone, *ibid*, p. 37.

REFERENCES

“Answering the Big Questions about New Nuclear Power Stations”, *EDF Energy*, <http://www.edfenergy.com/energyfuture/edf-energys-approach-why-we-choose-new-nuclear/implications-for-new-nuclear>, (Accessed on 02.08.2015).

BAYLON, C., “Drones: The Threat to Nuclear Plants”, *Newsweek*, 27 December 2014, <http://www.newsweek.com/drones-threat-nuclear-plants-294458>, (Accessed on 07.08.2015).

BAYLON C., BRUNT R., LIVINGSTONE D., “Cyber Security at Civil Nuclear Facilities-Understanding the Risks”, Chatham House, September 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

BISSON, D., “Korean Nuclear Power Plant Plans Cyber Attack Drills in Wake of Hacker Threats”, *Tripwire*, 22 December 2014, <http://www.tripwire.com/state-of-security/featured/korean-nuclear-power-plant-plans-cyberattack-drills-in-wake-of-hacker-threats/>, (Accessed on 07.08.2015).

BOLAND, B., “Networks on Fire: Defending Critical Government Networks”, *Cyber Security Some Critical Insights and Perspectives*, Damien D. Cheong (ed.), Nanyang Technological University S. Rajaratnam School of International Studies.

BOULANIN, V. and OGILVIE-WHITE, T., “Cyber Threats and Nuclear Dangers”, *Asia Pacific Leadership Network for Nuclear Non-Proliferation and Disarmament, Centre for Nuclear Non-Proliferation and Disarmament*, Policy Brief No. 17, November 2014, <http://www.a-pln.org/sites/default/files/apln-analysis-docs/Policy%20Brief%20No%2017%20-%20Cyber%20Threats%20and%20Nuclear%20Dangers.pdf>, (Accessed on 02.08.2015).

BROWNE, D. and IVANOV. I. S., “From Nuclear Safety to Nuclear Security”, *Project Syndicate*, <http://www.project-syndicate.org/commentary/nuclear-security-fukushima-by-des-browne-and-igor-ivanov-2015-03>, (Accessed on 24.08.2015).

CAŞIN, M. H., “The Future of NATO and Atlantic Security after the 2014 Wales Summit”, in *Geopolitics of the Caspian Region*, Ahmet Yükleyen (ed.), (Istanbul: Hazar Strategy Institute, 2015).

COFLIN, M. “Droning on Over Nuclear Power Plants”, *United States Nuclear Regulatory Commission*, 23 April 2015, <http://public-blog.nrc>

<http://gateway.gov/2015/04/23/droning-on-over-nuclear-power-plants/>, (Accessed on 10.08.2015).

COLLINS, S., MCCOMBIE, S., "Stuxnet: The Emergence of a New Cyber Weapon and Its Implications", *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, April 2012.

Cyber Security Strictly Regulated by NRC; No Additional Regulation Needed", *Nuclear Energy Institute Policy Brief*, March 2014,
<http://www.nei.org/CorporateSite/media/filefolder/Backgrounders/Policy-Briefs/CyberSecurity-Regulation-Strictly-Regulated-by-NRC-March-2014.pdf?ext=.pdf>, (Accessed on 07.08.2015).

"Cyber Security at Civilian Nuclear Facilities",
http://www.nap.edu/openbook.php?record_id=18412&page=72, (Accessed on 10.08.2015).

DEUTCH, J., FORSBERG, C. W. , KADAK, A. C. , KAZIMI, M. S. , MONIZ, E. J. and PARSONS, J. E. "Update of the MIT 2003 Future of Nuclear Power," *MIT Energy Initiative*, 2009, <http://web.mit.edu/nuclearpower/pdf/nuclearpower-update2009.pdf>, (Accessed on 31.07.2015).

DICK, R. L., Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation Before the House Committee on Governmental Reform, Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee Washington, DC", 24 June 2002, <https://www.fbi.gov/news/testimony/cyberterrorism-and-critical-infrastructure-protection>, (Accessed on 03.08.2015).

DUDENHOEFFER, D. D., "Office Of Nuclear Security Cyber Security Programme", *International Atomic Energy Agency*,
https://www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-2/4.cyber_security_introduction.pdf, and "Computer Security at Nuclear Facilities - IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual", http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf, (Accessed on 24.08.2015), 2011.

DUYEON K., JUNGMIN K., "Where Nuclear Safety and Security Meet", Bulletin of the Atomic Scientists, Vol. 68, 2012.

FLORY, D., "International Conference Cyber Space, Energy & Development: Protecting Critical Energy Infrastructure ITU Headquarters, Geneva", 10 October 2014, <http://www-ns.iaea.org/downloads/coordination/ddg/2014/itu-geneva-10oct2014.pdf>, (Accessed on 02.08.2015).

FULGHUM, D. A., "Why Syria's Air Defences Failed to Detect Israelis," Aviation Week, Ares Blog, 3 October 2007.

HERBACH, J. "Developing the International Law Framework to Better Address Cyber Threats: Role of Non-Binding Instruments", *Centre for Conflict and Security Law, University of Amsterdam*,
http://conflictandsecuritylaw.org/web_documents/j_herbach_developing_the_international_law_framework_to_better_address_cyber_threats.pdf, (Accessed on 23.08.2015).

HOLT, M. and ANDREWS, A., "Nuclear Power Plant Security and Vulnerabilities", *Congressional Research Service*, 3 January 2014,
<https://www.fas.org/sgp/crs/homesec/RL34331.pdf>, (Accessed on 01.08.2015).

International Atomic Energy Agency Board of Governors General Conference, "Nuclear Security – Measures to Protect Against Nuclear Terrorism Amendment to the Convention on the Physical Protection of Nuclear Material - GOV/INF/2005/10-GC(49)/INF/6 Date: 6 September 2005",
<https://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf>, (Accessed on 23.08. 2015).

"International Response Needed for Cyber Security Threats to Nuclear Facilities", 2 July 2015, <http://www.canadianunderwriter.ca/news/international-response-needed-for-cybersecurity-threats-to-nuclear-facilities/1003654812/?er=NA>, (Accessed on 05.08.2015).

JON R. L., "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, Vol. 22, 2013.

LO, C., "Nuclear Plant Operations: Unlocking the Human Factor", 26 February 2015, <http://www.power-technology.com/features/feature-nuclear-plant-operations-unlocking-the-human-factor-4516904/>, (Accessed on 13.08.2015).

LOPEZ, L. B., "Cyber Threats Put Energy Sector on Red Alert", *The Hill*, 15 July 2014, <http://thehill.com/policy/energy-environment/212220-cyberthreats-put-energy-sector-on-red-alert>, (Accessed on 02.08.2015).

MANNA, G., "Human and Organizational Factors in Nuclear Installations: Analysis of Available Models and Identification of R&D Issues", *European Commission Joint Research Centre Institute for Energy – Scientific and Technical Reports*, <http://iet.jrc.ec.europa.eu/senuf/sites/safelife.jrc.ec.europa.eu.senuf/files/files/documents/eur-23226.pdf>, (Accessed on 14.08.2015), 2007.

MARTELLINI M., "Cyber Security for Nuclear Power Plants", US State of Department, Washington, DC, January 2012, <http://www.state.gov/t/isn/183589.htm>

MELZER, N., "Cyber Warfare and International Law", *UNIDIR Resources*, 2011, <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>, (Accessed on 02.08.2015).

MORGAN H., "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment", Engineering Management Journal, Vol. 25, No.2, 2015.

NAKASHIMA, E., "U.S. Accelerating Cyber Weapon Research," Washington Post, 18 March 2012.

NIKISHIN, A., "ICS Threats: A Kaspersky Lab View, Predictions and Reality", http://campaigns.codenomicon.marketing/hubfs/CodenomiCON_Asia15 - Andrey_Nikishin.pdf?t=1438746812613, (Accessed on 03.08.2015).

North Atlantic Treaty Organization, "Wales Summit Declaration Issued by the Heads of State and Government participating in the Meeting of the North Atlantic Council in Wales 05 September 2014, *Press Release*, Issued on 5 September 2014, Last updated: 31 July 2015, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Accessed on 24.08.2015), 2015.

Nuclear Energy Institute-NEI Fact Sheets, "Nuclear Power Plant Security", September 2014, <http://www.nei.org/master-document-folder/backgrounders/fact-sheets/nuclear-power-plant-security>, (Accessed on 10.08.2015).

NYE, J. S., "From Bombs to Bytes: Can our Nuclear History Inform our Cyber Future?", Bulletin of the Atomic Scientists, Vol. 69, No. 5, September/October 2013, <http://thebulletin.org/2013/september/bombs-bytes-can-our-nuclear-history-inform-our-cyberfuture>, (Accessed on 01.08.2015).

OECD-Nuclear Energy Agency, "The Human Factor in Nuclear Power Plant Operation", No. 2, January 1988, <https://www.oecd-nea.org/brief/brief-02.html>, (Accessed on 13.08.2015).

PEDERSON, P., "Regulating Nuclear Cyber Security: The Core Issues: An Analysis of Existing Regulatory Frameworks in Light of the Increasing Cyber Threat against Critical Infrastructure", *The Langner Group*, Washington DC, January 2015, <http://www.langner.com/en/wp-content/uploads/2015/01/Regulating-Nuclear-CyberSecurity.pdf>, (Accessed on 03.08.2015).

WOO, T. H., "Nuclear Safeguard Protocol (NSP) Construction of Energy Policy in Nuclear Power Plants (NPPs) for Secure Power Production", Energy Sources, 2015, Part B, Vol. 10, No.1, 2015.

World Nuclear Association, "Safety of Nuclear Power Reactors", Updated July 2015, <http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Safety-of-Nuclear-Power-Reactors/>, (Accessed on 31.07.2015).

The Council of Europe, "Convention on Cyber Crime", Budapest, 23 November 2001, <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>, (Accessed on 23.08.2015).

"The Risk of Nuclear Terrorism from Insider Threats", *Bulletin of the American Academy of Arts & Sciences, Projects and Activities*, Summer 2014, https://www.amacad.org/multimedia/pdfs/publications/bulletin/summer2014/bulletin_Summer2014_InsiderThreats.pdf, (Accessed on 05.08.2015).

TRIPATHI, S., "Cyber: Also a Domain of War and Terror", *Strategic Analysis*, Vol. 39, No.1, 2015.

"United Nations - International Convention for the Suppression of Acts of Nuclear Terrorism -2005", <http://www.un.org/en/sc/ctc/docs/conventions/Conv13.pdf>, (Accessed on 23.08 2015).

U.S. Department of State Bureau of International Security and Nonproliferation, "Convention on the Physical Protection of Nuclear Material - Signed in New York, 3 March 1980, Entered into force on 8 February 1987", <http://www.state.gov/t/isn/5079.htm#treaty>, (Accessed on 23.08. 2015).

U.S. Department of State 01/23/12 Paper - Cyber Security for Nuclear Power Plants, "Cyber Security for Nuclear Power Plants Prepared by Maurizio Martellini, Thomas Shea, and Sandro Gaycken", January 2012, <http://www.state.gov/t/isn/183589.htm>, (Accessed on 10.08.2015).

WALKER, J. S., "Regulating against Nuclear Terrorism: The Domestic Safeguards Issue, 1970-1979", *Technology and Culture*, Vol. 42, No. 1, January 2001.

WEBB, G., "Experts Conclude Meeting to Discuss "Human Factors of Nuclear Safety", 27 May 2013, <https://www.iaea.org/newscenter/news/experts-conclude-meeting-discuss-human-factors-nuclear-safety>, (Accessed on 14.08.2015).

WEIMANN, G., "Cyber Terrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism*, Vol. 28, Issue 2, 2005.

CHARTING CRITICAL ENERGY INFRASTRUCTURES DEPENDENCIES ON SPACE SYSTEMS – NEW FRONTIERS IN RISKS, VULNERABILITIES AND THREATS

**Dr. Liviu MUREŞAN, Alexandru GEORGESCU
Ştefan POPA, Ştefan-Ciprian ARSENI
Iulia JIVĂNESCU**

ABSTRACT

Space systems are critical enablers of a wide range of applications utilized by a global range of consumers. Their consequent vulnerability is a critical issue affecting the security of critical infrastructures, in the context of increasing global interdependencies. This paper will argue that many categories of Critical Energy Infrastructures are uniquely dependent on a wide array of services provided by space systems, not just in their daily operation, but also in the very important issue of crisis and emergency situation management. The long-term trend is for these dependencies to grow, increasing the exposure of Critical Energy Infrastructures to the risk of space system disruption. This means that decision makers and competent authorities must become aware of these vulnerabilities and introduce them to the security calculus. The issue of protection is complicated by the transnational character of many Critical Energy Infrastructures and Critical Space Infrastructures.

Key Words: Space Systems, Critical Dependence, Risk Governance, Disaster and Emergency Situation Management

Introduction

Critical Energy Infrastructures (CEI) are a fundamental component of the infrastructure system-of-systems, on which the economic, social and political dimensions of an advancing and advanced society are based. Without a constant supply of electricity and other forms of energy, critical infrastructure systems such as transport, information and communication technology, health, food supply, and the many others identified under the European Program for Critical Infrastructure Protection⁴⁷¹ could not function,

⁴⁷¹ European Commission, “Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure”, 2013,

or, in the event of an intermittent or uncertain supply, could not function at the level required to maintain business continuity and quality of life. The purpose of this paper is to highlight the growing links between CEI and space systems, a complex relationship that is continually evolving in line with the needs of the CEI and the capabilities of the space systems.

These systems, mostly satellites, have become a key enabler for various applications on Earth, translating capabilities such as communications, remote sensing, navigation, positioning, timing and other specialized tasks into critical services such as command, control and coordination of complex systems and operations, information gathering in support of decision making, emergency situation and crisis management and a host of other services. The degree of involvement of space systems in the proper functioning of critical terrestrial infrastructure systems, from energy to transport and finance, has reached the point where certain space assets can be said to have achieved criticality (i.e. being of the utmost importance for the proper functioning and security of a system).⁴⁷² This means that space systems themselves are becoming critical infrastructures, systems whose disruption and destruction entail significant risk and damage.⁴⁷³ This has not gone unnoticed by the countries which are most advanced in the processes of critical infrastructure protection, namely Western countries or the most powerful emerging economies. We are undergoing a period in which the formal research of the nature and extent of the dependence of terrestrial critical infrastructures (CI) on critical space infrastructures (CSI) is becoming a priority. Concurrently, there are drive update reference materials, modes of thought and organization, competent security actors, and CI stakeholders (owners/administrators/operators of CI, as well as the elements of academia, government and civil society which take an interest in the proper running and protection of CI) to reflect these new developments.

CEI are extraordinarily complex, bringing together multiple component systems operating in sync, from energy extraction and refining to electricity production, transport and delivery to end consumers. They also have parallel systems that interconnect at key points, lending even greater complexity to the energy system-of-systems. For instance, electricity may be generated through different production chains (hydrocarbon, renewables, nuclear), which then come together on the grid for delivery to users. Space services also play a role in ensuring the coordination and smooth functioning of such a complex system. Over time, as certain factors such as increased reliability, decreased costs and increased capabilities come into play in the space industry, we may find that CSI become key components of terrestrial CI in many instances, though especially as an upper layer of command, control, coordination and

https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf , (Accessed on 10.11.2015).

⁴⁷² Wayne Klotz, et al., "Guiding principles for the Nation's critical infrastructures", *American Society of Civil Engineers*, 2009.

⁴⁷³ Kathryn Gordon and Maeve Dion, "Protection of critical infrastructure and the role of investment policies relating to national security", Investment Division of the Directorate for Financial and Enterprise Affairs, *Organisation for Economic Co-operation and Development*, 2008.

information gathering capabilities. Over the course of this paper, we shall further describe the particularities of space systems, provide a general overview of the services rendered to CEI and assess their criticality, present a case study on the dependence of the nuclear industry on space services, and finally, describe the risk profile of CSI, arguing that new risks, vulnerabilities and threats are emerging from increasing reliance on space systems.

It is especially important to remember that increasing dependence on space systems, especially in areas termed critical, generates new risks. Ensuring the resilience of a society or a particular critical infrastructure system such as energy (where resilience is the ability of a system to recover to adequate capacity from a disruption or negative event with minimum damage in the fastest amount of time)⁴⁷⁴ requires a specific understanding of space systems. On this understanding, space systems are not just providers of services for emergency and crisis management (which increases resilience), but as originators of specific security threats related to their characteristics and their environment.

Critical Space Infrastructures

Since the launch of the Sputnik satellite which established mankind's presence in space, there has been a continuous drive towards the development of new capabilities for space systems, enhancing the accuracy, capacity and reliability of existing capabilities and increasing the number of space assets that can provide these services. The satellites that are most likely to provide critical services are communication satellites, Earth Observation satellites (weather monitoring, analysis of terrestrial conditions and phenomena) and global navigation satellite systems (GNSS such as GPS, GLONASS, GALILEO, the Chinese BEIDOU and a host of regional systems). As an extension to the CSI, there are also ground stations that provide communication links or augment the capacity of the space system in some way, such as increasing the positioning accuracy of GNSS.

One can describe, informally, the development of space systems into CSI by noting their widespread use in transport, in facilitating and coordinating financial markets (GNSS, in particular, is important for timestamping transactions) or in aiding decision makers during emergency situations and crises. CSI serve tens of millions of users and, ultimately, impact billions of beneficiaries, mostly from developed countries (which are at the technological and productivity frontier). Increasingly, however, developing countries are skipping certain stages of development through space systems (i.e. switching directly to satellite communications and the Internet instead of creating physical, ground-based national communication networks).

Another way to highlight the extraordinary development of CSI, and, accordingly, to infer the increasing reliance on them is to analyze the growth of the space and satellite industry. The 2015 State of the Satellite Industry Report, commissioned by the Satellite

⁴⁷⁴ Myriam Dunn Cavelty and Tim Prior, "Resilience in security policy: present and future: CSS Analysis in Security Policy", No. 142, 2013, *Center for Security Studies*, ETH Zurich.

Industry Association, states that in 2014, the overall revenue of the satellite industry grew by 4%, outstripping global growth. This is impressive given the economic crisis that began in 2008. Overall, industry revenues have grown by 130% compared to 2004. Some areas, such as mobile data services, have seen yearly growth rates of 25%.⁴⁷⁵ Due to greater competition in launch services, a steady fall in the launch costs and the advent of new technologies such as CubeSats and better instruments that do not require the same extensive satellite platforms to offer commercial grade services, 208 new satellites were launched in 2014. Of these, 63% were CubeSats, as opposed to 107 in 2013. There are also factors driving this trend and maintaining growth, including: greater competition leading to lower launch costs; the fact that the cost of new assets will decrease following new design philosophies such as modular satellites, life extension capabilities, technological development and economies of scale; and the scope for reducing insurance and financing costs through a better understanding of the security environment, further opening the industry to new actors and new applications. One should also note the slow but steady development of a better framework for the commercial exploitation of space under more predictable conditions (better global governance of the space environment, international organizations stewarding the global space commons and managing scarce resources such as access to the most profitable orbits or access to the bandwidth spectrum for telecommunications, new international legislation, and an adaptation of existing commercial law and customs to space, including for potential liability). Finally, we are already seeing the emergence of new business models for more affordable access to space services, such as the European Space Agency's Copernicus (formerly GMES) program, which features an open-source data model for the data gathered by the Sentinel satellites.⁴⁷⁶

Space Applications for Energy Infrastructures

As mentioned earlier, CEI are composed of varied systems that must work together. The propagation of risk throughout this system-of-systems is a real possibility, as is that of cascading disruptions from an initial failure point throughout the entire CEI. Increasingly, these risks come from asymmetric threats, such as cyber attacks that generate "systemic shocks" that can wholly destroy or debilitate a critical infrastructure system.⁴⁷⁷ Given the seminal role of CEI in the functioning of almost every other critical infrastructure system, the emphasis placed on its protection by governments and other security actors is understandable. Space systems have become primarily a

⁴⁷⁵ Tauri Group, "2015 State of the Satellite Industry Report", commissioned by Satellite Industry Association, published September 2015, <http://www.sia.org/wp-content/uploads/2015/06/Mktg15-SSIR-2015-FINAL-Compressed.pdf> (Accessed on 10.11.2015).

⁴⁷⁶ European Space Agency, "Free access to Copernicus satellite data", 2013, http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Free_access_to_Copernicus_Sentinel_satellite_data (Accessed on 10.11.2015).

⁴⁷⁷ Sr. Capt. Bart Smedts, "Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (near) Future", Focus Paper 15, Center for Security and Defence Studies, *Royal High Institute for Defence*, 2010.

management and planning tool for the day-to-day operation and planning of CEI, as well as important instruments for managing crises and emergencies. The level of penetration of CSI into CEI varies from subsector to subsector and from region to region.

One might still have Industrial Revolution-era coal mining without space systems to monitor air quality, geological shifts, mineshaft integrity, environmental damage, etc. At the same time, transporting the coal to the end-user, especially as part of the global supply chains favored by energy-poor countries with energy intensive industries (such as China, India, Japan) entails the use of transport companies and port facilities. These use GNSS services for navigation, positioning, ensuring fluidity of traffic in chokepoints like channels and straits and proper port management for busy infrastructure. Then, after being converted to electricity, it is fed into the grid, which relies on communication networks between humans and automated systems, as well as the synchronization capacity of GNSS atomic clocks in order to maintain system integrity, especially if the electricity grid features a myriad of intermittent producers, like renewable sources of electricity.

Energy production significantly predates the advent of space systems, meaning that it has been possible for it to function correctly without space capabilities. The rate at which states and companies decide to utilize space systems conforms to their own internal calculus of security, cost, profitability and ultimate liability for the materialization of one of the numerous threats facing energy systems. For the most part, the trend seems to be towards greater reliance on space systems, especially for the aforementioned grid management, the complexity of which requires specialized management capabilities and real-time decision making. However, one should not discount the importance of communication and coordination upstream and downstream throughout the energy supply chain. This importance increases with the internationalization of this chain, meaning that global systems are more likely to utilize space capabilities in order to reduce uncertainty.

Because environmental awareness is an increasing concern for civil society stakeholders and national authorities, it has also become an important consideration for the owners/operators/administrators of CEI. Remote sensing capabilities provide real-time and permanent monitoring of facility outputs such as pollutants in the air, soil or water. They can also analyze the impact of the resulting heat on the environment, providing regulators and decision makers with actionable data on the environmental impact of energy extraction, production, transport and so on.

Space capabilities have also been used to detect likely new deposits of fossil fuels for future exploration. With the most accessible deposits under exploitation reaching and surpassing the peak outputs, there is growing pressure to identify less accessible (and detectable) deposits deeper underground, or under the maritime continental shelf and even under ice caps. However, the concurrent increase in environmental awareness outweighs, in certain instances, economic pressure, leading to a push towards renewable sources of energy, which are fundamentally dependent on information

gathering in their planning stages. Space capabilities can offer immensely valuable information regarding local weather and climate, the expected amount of sunlight and wind, even the strength of the tides, identifying the best places to install renewable energy generation capacity. Their role in monitoring and predicting weather patterns also makes them invaluable in assessing the expected outputs of these systems and providing better coordination among all energy producers, across the system-of-systems, by giving advance warning of the likelihood of requiring reserve generation capacity to fill the gap left by intermittent sources.

As mentioned above, crisis and emergency situation management is one area where space systems are rapidly becoming ubiquitous, due to the advantages they offer. The coordination of the electricity grid in case of an incident affecting one or more producers is one such example. Another is the diagnosis of problems and the coordination of field repair teams, or the containment of hazardous substance spillovers. The use of space capabilities enhances not only CEI resilience, but also its robustness and adaptability. These are all concepts used in association with resilience, to describe the various dimensions of a resilient system.⁴⁷⁸ Another way of viewing the strength of a system augmented by CSI is to consider its resilience in terms of its restorative, absorptive, and adaptive capacities.⁴⁷⁹ All of these are served, in one way or another, by space capabilities.

In large part, the most important space systems for CEI are GNSS, communication satellites and various providers of Earth Observation data. The rate at which these systems are adopted indicates the technological sophistication of the company or society in question. Once adopted, CSI are invaluable not only to the daily operation of the system, but also for managing potential disruptions. Even if there are no space systems that could be considered critical to the proper functioning of a certain regional or National CEI, this does not mean that there is no critical dependency path that could affect CEI.

Critical infrastructure protection theory advances the idea of powerful interconnections between the various critical infrastructures, leading to the propagation of risks, vulnerabilities and threats, as well as the possibility of cascading disruptions. CEI are a basis for other infrastructures, but interconnectivity is a two-way relationship.⁴⁸⁰ Viewed in the context of CSI dependence, this means that, even in the absence of direct dependence, CEI will register a certain exposure to CSI through its involvement in other terrestrial critical infrastructures on which it is dependent. This indirect

⁴⁷⁸ Per Hokstad, Ingrid Utne and Jørn Vatn, "Risk and Interdependencies in Critical Infrastructures", *Springer Series in Reliability Engineering*, Springer, Trondheim, Norway, 2012, pp. 16-18.

⁴⁷⁹ Eric Vugrin, Drake Warren and Mark Ehlen, "A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane", Sandia National Laboratories, *6th Global Congress on Process Safety*, 2010.

⁴⁸⁰ Adrian Gheorghe and Markus Schläpfer, "Critical Infrastructures: Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures", *IRGC - ETH Document*, 2004, Zürich.

relationship may entail secondary dependence or even tertiary dependence, via the effect of CSI on an infrastructure on which another infrastructure related to CEI is dependent, or on the infrastructures across an entire geographic area. Such interdependencies have been described for terrestrial CI,⁴⁸¹ but they are now also being defined in relation to CSI. All of these relationships exist concurrently, and provide the significant complexity of critical infrastructure interaction, not just as technical systems, but also socio-technical systems, with an important human and organizational element.⁴⁸² To illustrate, we can return to the previous example of the international transport of coal to the consumer, and the dependence of this system on GNSS. This is a point where CEI are critically dependent on critical transport infrastructure, and indirectly dependent on GNSS. Another example is the construction of CEI, a very expensive undertaking which requires a developed financial market to attract the required capital and financial instruments such as insurance, hedging on electricity or fossil fuel prices, and so on. These, in turn, are dependent on GNSS for transaction timestamping, on communications for international market coherence, and on the synchronization and integrity of databases etc.

One final service performed by a special class of space systems is to warn against a highly dangerous phenomenon, specific to space – “space weather”. This affects not only satellites but also energy systems. Despite the name, it has nothing in common with terrestrial weather patterns; rather it refers to the high-speed ejection of solar plasma, charged particles, radiation and other hazards that bombard the Earth. Their effects can be catastrophic, not only on space systems - which feature significant vulnerabilities that will be discussed in a later section - but also on terrestrial energy systems. The most powerful solar storm ever recorded took place in 1859 and was dubbed the Carrington Event, after British astronomer Richard Carrington, who monitored it. The storm caused auroras to appear on the Equator, telegraph poles to catch fire and telegraph lines to work without a source of electricity. Human vulnerability to such events has increased year on year, especially since the advent of vulnerable microelectronics. The electromagnetic pulse effect of various nuclear bomb tests has also demonstrated the vulnerability of technologically advanced societies in the face of space phenomena. Though a Carrington event has not been repeated (they have taken place, but on the far side of the Sun, there have been lesser storms whose effects underline this dramatic vulnerability. The solar storm of 13–14 September 1989, one of the largest ever recorded, left 6 million inhabitants of the Canadian province of Quebec without electricity for several hours and caused many planes to be grounded

⁴⁸¹ Adrian Gheorghe, Sara Marie Bouchon and Jurg Birchmeier, “Toward Guidelines for Regional Assessment of Vulnerability against Service Disruption of Critical Infrastructures”, *EsReDa*, the 29th Seminar “System Analysis for a More Secure World” Proceedings, 2006, pp. 81-95.

⁴⁸² Adrian Gheorghe, Marcel Masera, Margot Weijnen and Laurens De Vries, “Critical Infrastructures at Risk - Securing the European Electric Power Systems”, *Springer Netherlands*, 2006.

or rerouted, as well as the impact on space equipment.⁴⁸³ The 2003 “Halloween storm” was another peak of solar activity,⁴⁸⁴ which saw power disruption for millions of people on the ground. In addition, orbital activity was seriously affected – a number of satellites were lost, 59% of scientific missions were interrupted and astronauts had to take refuge in specially shielded areas of the International Space System.⁴⁸⁵

The National Oceanic and Atmospheric Administration (NOAA) is a US agency charged with researching and monitoring natural phenomena which can disrupt American air and maritime activity. Its remit has now been extended into space, and it has created a series of charts classifying the effects of various space weather phenomena in order of severity. With regard to the critical energy infrastructures, NOAA scales⁴⁸⁶ regarding geomagnetic storms indicate that the first fluctuations in energy grids appear even for G1 events (the least dangerous) and grow in severity. During a G3 event, noticeable challenges appear for grid operators, with false alarms and equipment damage. At the highest level, G5 events can cause the partial or total collapse in the grid, with significant damage to transformers.

A report by the US National Research Council (NRC) estimated that if a Carrington event were to take place today and strike a very advanced region of the Earth, the resulting damages would be valued at \$2 trillion in the first year for the US alone, with full recovery time estimated at 4-10 years.⁴⁸⁷ In addition, there would be significant secondary and tertiary losses from effects on partners in Europe. Other key terrestrial infrastructures, such as land-based communication systems, the computer, database and communication links on which the financial system is built, along with any other infrastructure dependent on a reliable supply of electricity and communications would also be disrupted. Existing weak links in infrastructure systems, due to differences in the age of systems, lack of maintenance etc., would be harnessed to inflict even greater damage. The NRC has estimated that due to vulnerable and aging transformer stations, over 130 million consumers in the US alone would be deprived of electricity for more than a few hours.⁴⁸⁸ In addition to simply disrupting the energy grid, geomagnetically induced currents can have other more insidious effects. For instance, they can disrupt the weak currents preventing the corrosion of energy pipelines or disrupt vital grid equipment, such as compensators, which prevent voltage collapse,

⁴⁸³ Royal Academy of Engineering, “Extreme Space Weather: Impacts on Engineered Systems and Infrastructure”, London, 2013.

⁴⁸⁴ M. Weaver et al., “Halloween Space Weather Storms of 2003”, NOAA Technical Memorandum OAR SEC -88, NOAA, 2004.

⁴⁸⁵ Yousaf M. Butt, “The EMP threat: Fact, Fiction, and Response”, <http://www.thespacereview.com/article/1553/1>

⁴⁸⁶ Space Weather Scales, NOAA Space Weather Prediction Center, <http://www.swpc.noaa.gov/NOAAscales/> (Accessed on 23.09.2015).

⁴⁸⁷ National Research Council, “Severe Space Weather Events: Understanding their Economic and Societal Impact”, Workshop Report, Washington DC, 2008, <http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf>, (Accessed on 23.09.2015).

⁴⁸⁸ Ibid., pp. 3-78.

making grid management even more difficult and increasing the odds that a local blackout will turn into a national one. This happened in Malmö, Sweden in 2003.⁴⁸⁹

This is where space systems come into play. For example, the most important “warning flag” for solar storms is NASA’s Advanced Composition Explorer (ACE) launched in 1997, which can give advanced warning 15 or 45 minutes before a front of solar activity reaches Earth. Other satellites dedicated to solar monitoring include the Solar and Heliospheric Observatory (SOHO), DSCOVR, STEREO A and B, IRIS, WIND, and the Solar Dynamics Observatory (SDO) from NASA, Hinode (Japan Space Agency), Solar Orbiter, Proba 1 and 2 from the ESA. There are also a number of satellites performing other missions that are equipped with radiation monitors and other relevant instruments.

The availability of data has led to the appearance of various notifications and early warning services⁴⁹⁰ to which important infrastructure operators can subscribe to receive advance notification of an event and implement preventative measures, such as a system shutdown. Further research into this field has yielded knowledge regarding the hardening of CEI systems against space weather, and the recurrence of these events provides an added incentive for the implementation of such measures.

To sum up, reliance on space systems on the part of CEI is highly contextual, depending on the subsector in question, the characteristics of the economic operator in charge of the subsector, relevant national and regional (European) legislation, incentives for the adoption of space capabilities, and the phase of CEI activity in question (space capabilities are more likely to be used in an emergency).

Case Study – Nuclear Industry

Since civilian and military nuclear applications pre-date the important technological developments that have enabled an increasingly critical role for space systems, the instances in which space applications are truly critical for the functioning of the Nuclear Industry are limited. They are used in a complementary fashion, but are also emerging as powerful instruments in the increasing security apparatus surrounding all facets of the Nuclear Industry, not only the production of energy, but also the mining, refining and transport of nuclear material; the disposal of nuclear waste, which is a permanent responsibility; proliferation of nuclear technology and its development along military lines; handling of public perceptions of security governance in the field; and security governance efforts, especially from human and environmental perspectives.

The critical dependence of the Nuclear Industry on space systems is mostly limited to its important role in effective crisis and emergency situation management, as well as the secondary and tertiary influences registered through the Nuclear Industry’s dependence on other CI systems, which may be more dependent on CSI (as explained

⁴⁸⁹ Royal Academy of Engineering, “Extreme Space Weather: Impacts on Engineered Systems and Infrastructure”, London, 2013, p. 22.

⁴⁹⁰ Mike Hapgood, Alan Thomson, “Space weather and its impact on Earth and implications for Business”, *Lloyd’s 360 Risk Insight Briefing*, 2010, p. 22.

in the previous section). In general, the most important space services for the Nuclear Industry will be synchronization, communications and Earth Observation, with differences in criticality based on subsector, circumstances and the availability of substitutes for these services.

Often, the criticality of a space system to a CI, including to the Nuclear Industry, will only become apparent if the CSI in question malfunctions at precisely the worst possible moment; a key example is the Japanese ALOS Earth Observation satellite, which malfunctioned just as the Fukushima disaster demanded all resources in intelligence gathering.

A possible classification of the uses of space systems as instruments in the Nuclear Industry's toolbox, especially its security apparatus, places three of them in direct connection to Nuclear Industry as an energy producer, while the fourth, although not directly linked to the energy production, is nevertheless important in security governance processes.

- 1. The feasibility and environmental studies required for the approval of new reactors, as well as the security of the various nuclear industry processes*

As the demand for security governance in the field increases, with every new accident or incident resounding in the public imagination, so does the requirement that maximum diligence be applied in the selection of new sites to host nuclear facilities. This includes not just reactors, but also research centers, material mining, processing and enrichment facilities, as well as transport operations. The location of nuclear reactors is especially important, since their long timeline for exploitation requires that the environment itself minimizes the potential for catastrophic risks and disruptions, with the lowest possible impact on the environment and human settlements. An area afflicted by a nuclear meltdown might become unfit for human habitation, and weather patterns may carry radioactive fallout all over the world, including very densely populated areas. Therefore, extensive Earth Observation capabilities are used to study the geology of the site, the relief and its impact on the possible spread of nuclear fallout, the atmospheric phenomena and currents, the yearly weather patterns and a host of other factors. Most importantly, space system surveillance allows for permanent monitoring, as well as the accumulation of valuable historical data for study.

- 2. Permanent security for the waste disposal sites*

While this type of activity and facility within the Nuclear Industry could have been included in the category above, its importance warrants its separate consideration. Until applications are developed to manage highly radioactive nuclear waste - such as reactors that can use them as fuel - these materials will have to be permanently safeguarded against natural and human factors. The tens of thousands of years required for their dangerous levels of radiation to subside demand, for the foreseeable future, a permanent security apparatus to guard against accidental dispersions of materials, as well as theft by criminal and terrorist elements. Space systems, particularly Earth Observation satellites, but also communication satellites, allow for

better management of disposal sites at national levels, with coordination of rapid response capabilities to any threats. Of course, the selection of the waste disposal sites is subject to even more stringent criteria than that of nuclear reactors, with a preference for geologically stable and easily observable areas, far away from human habitation and difficult to reach.⁴⁹¹ Transport of nuclear waste which often involve multiple connections and international transits, also benefit from surveillance and coordination capabilities.

3. In every phase of a nuclear accident, in support of decision makers and investigators

The use of space systems for the management of crisis and emergency situations is already well established, since they provide command, control and coordination capabilities to responders on the ground, as well as information to specialists assessing the severity of the event and its evolution.⁴⁹² It was only natural that space capabilities would be compatible with the needs of nuclear accident responders and investigators. This was highlighted during the Fukushima disaster, when the Sentinel Asia initiative, to which Japan belongs, provided immediate surveillance of the affected area as the crisis unfolded. During this time, the main Japanese Earth Observation satellite involved, ALOS, was lost.⁴⁹³ Even though ALOS 2 and 3 have been launched, the Japanese have decided that redundancy and robustness in their Earth Observation capabilities is required, which is why a constellation of microsatellites developed by Japanese universities has been launched.^{494,495} It is interesting to note that these satellites were used not only during the Fukushima disaster and in the surveillance afterward, but also for researching the conditions at the Chernobyl NPP in Ukraine, due to increased Japanese interest in the site of the most famous meltdown and consequent total evacuation.

In addition to Earth Observation satellites, communications satellites were also used extensively to connect the authorities with command posts in cities, re-establish contact with the population, and coordinate anti-meltdown and evacuation efforts.

⁴⁹¹ Thomas Haeme, “Use of satellite and airborne remote sensing in the safeguards of a nuclear waste repository site”, “Safeguards for Final Disposal of Spent Nuclear Fuel - Methods and technologies for the Olkiluoto site”, Olli Okko (ed.), 2003, pp. 20-36.

⁴⁹² Committee on Earth Observation Satellites (CEOS), “Satellite Earth Observation for Disaster Risk Management” in “CEOS Earth Observation Handbook 2012 - Special edition for Rio+20”, 2012,

http://www.eohandbook.com/eohb2012/case_studies_satellite_earth_observation_for_disaster_risk.html

⁴⁹³ Airbus Defense and Space, “Space Resources for Stricken Japan”, <http://www.space-airbusds.com/en/news2/airbus-defence-and-space-satellites-observe-disaster-in-japan.html> (Accessed on 10.11.2015).

⁴⁹⁴ Takaaki Iwasa, “Disaster Monitoring Activities in Japan”, February 2012, <http://www.unoosa.org/pdf/pres/stsc2012/tech-11E.pdf> (Accessed on 12.11.2015).

⁴⁹⁵ Seiji Yoshimoto, et al., “Environment Monitoring of Fukushima and Chernobyl Areas using a Constellation of Earth Observation Microsatellites (Japan-Ukraine Cooperation Technical Demonstration Program for Supporting Aftermath Responses to Accidents at Nuclear Power Stations)”, 5th Nanosat International Symposium NSS-05-0104, 2013.

4. *For non-proliferation efforts and verifying nuclear compliance of problem states or other entities*

The Comprehensive Nuclear-Test-Ban Treaty (CTBT) was established to prohibit the detonation of nuclear weapons in the Earth's atmosphere, underground or underwater. It is of the utmost importance to control the proliferation of nuclear technology, which can be weaponized. Countries which have civilian nuclear sectors but are suspected of trying to become nuclear powers for geopolitical gain - despite having signed relevant disarmament treaties - must be continuously assessed for covert efforts toward nuclear militarization. The threat is not only that a state may obtain nuclear weapons and possibly a delivery system, although ad hoc delivery methods, such as covert transport, are liable to be more effective than intercontinental ballistic missiles or other elements of the "nuclear triad". There is also the possibility that non-state actors will obtain nuclear weapons, even in small quantities, which they will be more willing to use. According to numerous studies, including by the RAND Corporation, non-state actors are mostly immune to traditional deterrence logic, which based on the threat of mutually assured destruction. Non-state actors have no territory or population to worry about, and may even be hostile to the country on whose territory they are based. Also, their political goals are likely limited and well defined, which makes the persuasiveness of a single nuclear weapon very attractive.

For these reasons, the most important space systems for non-proliferation efforts are specialized Earth Observation satellites. However, the criticality threshold has not been reached, because the CTBT has an entire system at its disposal, to which space systems are a complementary addition, not yet critical but growing in importance. The main elements of the system are:⁴⁹⁶

- The International Monitoring System, which relies on seismic sensors, hydro-acoustic sensors, infrasound sensors for atmospheric and radionuclei detection stations, with satellite systems as a more recent addition. In all, the system has 321 monitoring stations and 16 research laboratories. The use of space systems does have a long history, despite their lack of centrality within the system. In 1970, American Corona satellites were used to assess the Russian and Chinese nuclear programs. Both the Russians and the Americans detected nuclear preparations by South Africa in the Kalahari Desert in the 1980s, and eventually persuaded the country to dismantle its military nuclear program. The same systems detected Indian tests in Rajasthan in 1995, and there are many more such examples.⁴⁹⁷
- The International Data Centre;

⁴⁹⁶ Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization, "Overview of the Verification Regime", <http://www.ctbto.org/verification-regime/background/overview-of-the-verification-regime/> (Accessed on 10.11.2015).

⁴⁹⁷ Vipin Gupta, Frank Pabian, "Viewpoint: Commercial Satellite Imagery and the CTBT Verification Process", *The Nonproliferation Review*, Vol. 5, No. 3, 1998.

- Consultation and clarification processes;
- The Global Communications Infrastructure – which mediates communications between the monitoring stations, the Data Centre, the national governments and so on, relying on six dedicated communication satellites and three ground centers;
- On-site inspections – which are justified beforehand by evidence, including data gathered by satellite, which also define the scope of the inspectors' activity;
- Trust-building measures – which also rely on satellites for non-intrusive general verification of adherence to agreements.

The use of satellite capabilities has grown for a number of reasons, beyond the general factors such as better costs and instrument sensitivity.⁴⁹⁸ From the perspective of compliance verifiers, satellites have a number of significant advantages. Firstly, they are passive detectors and non-intrusive, and thus do not infringe on the rights of those surveilled. Secondly, they allow for permanent monitoring, especially visual, and can justify further and more intrusive methods of verifying compliance, especially via early warning capabilities for a nuclear test. Unlike other means of detection, satellites can precisely pinpoint a test area, giving inspectors a valuable starting point. Finally, satellites also provide useful evidence of illicit nuclear activity to the public. The international public is more likely to be receptive to the message if presented with incontrovertible visual evidence of a build-up for a test or the post-testing landscape. The international community can then put pressure on the offending nation to reduce or renounce its nuclear ambitions. Satellites can also provide surveillance under sensitive conditions. Theoretically, it is not illegal to prepare for a nuclear test, just to perform one, and countries may try to mislead the international community with regards to the state of their nuclear program. Satellites allow for the detection of a range of activity, including anything outside the acceptable limits for the country's nuclear program.

This presentation of the applications of space capabilities in the Nuclear Sector illustrates the uncertainty around the critical status of space systems. It is obvious that the criticality fluctuates based on circumstances, increasing in crisis situations. In all other cases, there are already models and instruments performing some of the functions offered by space systems without a dependence on them, even though CSI offer convenience and regularity in surveillance. As long as their functions are easily substituted, without sacrificing efficiency, then the criticality of the CSI remains lower in the case of the Nuclear Sector, with the aforementioned exceptions. However, the factors behind the rapidly increasing dependence of terrestrial infrastructure systems on space critical infrastructures are also applicable in the case of the Nuclear Industry. The Nuclear Industry also has specific characteristics that serve to increase its dependence on CSI:

⁴⁹⁸ Vipin Gupta, Frank Pabian, "Viewpoint: Commercial Satellite Imagery and the CTBT Verification Process", *The Nonproliferation Review*, Vol. 5, No. 3, 1998.

- Deteriorating public perceptions of the nuclear industry, which will demand increasingly sophisticated and responsive security systems that are integrated with CSI, to govern normal activity and crisis situations in particular;
- The rapid development, through direct demand, but also independently, of new services with space components which may serve the needs of the nuclear industry. New instruments are devised and launched, their accuracy is increased, their output finds new applications or new interpretations, etc.;
- The growing dependence of other terrestrial CI on CSI will also translate into greater indirect effects on the Nuclear Industry, even if its own consumption of space services were to remain the same, which is unlikely. In particular, the Nuclear Industry registers significant inter-dependencies with the energy transmission sector, with transport infrastructures and with the financial and banking systems, all of which are classified as critical infrastructures in every framework devised, including the American and European ones.

Over time, we will see an increase in dependence on space systems, driven, in part, by the risk aversion of the public and the demands for efficiency in the handling of crisis situations, with minimal loss of life, mitigation of damage and rapid resumption of normal activity. In short, the public demands resilience, and space systems are a factor in ensuring this, while increasing its exposure to CSI specific risks.

The Risk Profile of CSI

We have advanced the idea that space systems now deserve to be classified as critical infrastructures. The quality of criticality means that their disruption or destruction would adversely impact the system that registers dependence on them. For this reason, it is very important to describe the risk profile of critical space infrastructures, especially since there are significant differences with most of their terrestrial counterparts.

For one, CSI operates in one of the most extreme environments known to man, full of debris shooting around at hypervelocity, extremes of temperature and exposure to radiation, particles and plasma. This means that in addition to concrete risks, there is an ever-present threat of spontaneous malfunction or degradation in operational parameters. The economic and technical barriers to space exploitation, which might be alleviated over time, lead to several important consequences. Weight is limited and extra shielding entails a trade-off in functionality and on-board fuel (which enables course corrections that extend the operational lifetime of a satellite). Consequently, most civilian satellites are frail in comparison to military ones (but even then, the militaries of space-faring nations are not so lucky, since their needs surpass the capacity of military satellites – for instance, 90% of US military communications are routed through civilian satellites).⁴⁹⁹ Most satellites are designed for a specific mission,

⁴⁹⁹ Ian Easton, “The Great Game in Space: China’s Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy”, *Project 2049 Institute*, 2009, p. 8,

leading both to high unit costs and reduced ability to interface with other satellites and supplement their capabilities in case of need. Most satellites are not designed with significant redundancies or extra capacity, and replacing them is expensive and time-consuming. The satellite constellations created by government authorities, like the various GNSS networks, are planned with redundancies in mind, in the form of extra units. One of these, the European GALILEO system, is even compatible with the American GPS and the Russian GLONASS, and therefore can use them to boost service quality⁵⁰⁰. Most systems do not have such a degree of interoperability.

All of this means that the millions of users and billions of beneficiaries of space services are actually served by a very low number of space assets, compounding the risks associated with disruption in the provision of services by one or more satellites. According to an open-source database maintained by the Union of Concerned Scientists,⁵⁰¹ there are only 1,305 known satellites, of which 549 belong to the US, 131 to Russia and 142 to China. Of the 549 American satellites, 250 are commercial, 21 civil, 126 governmental, and 150 military. This is a relatively small number of satellites for the breadth of capabilities and the number of beneficiaries.

A departure from the status of most terrestrial critical infrastructures is the international nature of the space environment. While satellites remain under the sovereignty of the nation that launched them or of the company that commissioned them, space is a difficult environment for risk and security governance. Sovereignty over national airspace does not extend into space itself, and the orbital dynamics of satellites (aside from geostationary ones) results in them passing over numerous countries and regions several times a day. A framework for space governance is carefully being formed to govern critical aspects of the “orbital commons”. A series of international treaties, organizations and non-governmental actors are working to plug the gaps in the framework for space governance in order to prevent potential conflict and its attending risks, in order to encourage more private actors to invest in the field and in order to manage scarce resources.

The most valuable narrow orbital bands are the ones that take satellites over the most profitable markets. Therefore, even though outer space is very large, in practice satellites pass very close to one another and even collide with each other or with deactivated units or debris from time to time. This leads to one of the space-specific threats – collisions with space debris, which can be even very small natural or artificial debris whose speed can completely obliterate a satellite or even pose a threat to human missions. For instance, the active NASA UARS satellite was destroyed and the Meteosat 8 satellite was expelled from its orbit, both by powerful impacts. Then, in

http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf
(Accessed on 15.09.2015).

⁵⁰⁰ European Space Agency Website,
http://www.esa.int/Our_Activities/Navigation/Galileo_and_EGNOS (Accessed on 5.11.2015).

⁵⁰¹ Union of Concerned Scientists, *Open-Source Satellite Database Statistics*,
<http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.Vg0BUCvkVTB> (Accessed on 30.06.2015).

February 2009, an American commercial satellite, Iridium 33, collided with a Russian military satellite, Kosmos 225, at the speed of 11.7 km/s.⁵⁰² The number of traceable debris fragments generated by the incident was over 2,000, with thousands more too small to trace. A representative from Iridium Corporation, which runs a 66 satellite constellation, stated that the corporation receives hundreds of weekly close proximity warnings, issued when one of its satellites passes within 5 km of another satellite, and Iridium 33 was scheduled to pass the non-functioning Russian one by just 584 meters.⁵⁰³ The United Nations Committee on the Peaceful Uses of Outer Space is developing technical standards and recommendations aimed at minimizing the rate of production of new debris in one of the least regenerative environments known to man, both by de-orbiting satellites at the end of their useful lifespan, and by minimizing the debris resulting from launches. In the future, measures could be taken to actively clean orbits of debris, especially those where natural re-entry into the atmosphere takes years.

Even the radio spectrum for communications is limited, and is governed by the International Telecommunication Union, which ensures that satellites passing close to one another do not have similar frequencies - otherwise they may jam each other. The Center for Developments, Concepts and Doctrine within the Ministry of Defense of Great Britain published a report warning against "frequency fratricide", both unintentional and deliberate. This has happened several times before - the Galaxy 15 satellite stopped answering commands for about 4 months, in 2010;⁵⁰⁴ in 1998, Galaxy 4, situated in geostationary orbit, was similarly affected, leading to the loss of functionality of 90% of pagers in the US and problems with TV broadcasts for a few days.⁵⁰⁵

The second space-specific threat is "space weather", to which space systems are uniquely vulnerable, as described above. Here, too, there are proposals to protect satellites against radiation and to provide backup capacity in case anything should happen.

Finally, there are human threats to space systems, compounded by the predictability of a satellite's route through space. A wide variety of anti-satellite weaponry has been developed, including ASAT missiles. The main threat, however, does not come from space-faring nations with sophisticated militaries, which balance the threat of mutually assured destruction should they commence anti-satellite operations. For instance, China's ASAT missile test on FengYun-1C in January 2007 created 12% of the existing

⁵⁰² Brian Weeden, "Billiards in Space", *Space Review*, 2009, <http://www.thespacereview.com/article/1314/1> (Accessed on 20.09.2015).

⁵⁰³ Thomas Sean Kelso, "Iridium 33/Cosmos 2251 Collision", *Center for Space Standards and Innovation*, Colorado Springs, USA, 2009.

⁵⁰⁴ "Space: Dependencies, Vulnerabilities and Threats", Section 4-8, Centre for Developments, Concepts and Doctrine, Ministry of Defence, United Kingdom, 2012.

⁵⁰⁵ Steven Rinaldi, James Peerenboom and Terrence Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine*, Vol. 21, No. 6, 2001, pp. 11–25.

orbital debris in a single strike, increasing the perception of space as a veritable minefield.⁵⁰⁶ Given the critical nature of many satellite systems, and the degree to which their scarcity means that even potentially rival nations depend on the same systems, a space war is unlikely, according to a RAND Corporation report.⁵⁰⁷ Rather, it is non-state actors (terrorists, organized crime groups) and rogue states that have witnessed the most development in affordable anti-satellite weaponry – cyber-warfare, jamming, laser blinding and so on. All of these possibilities emphasize the gap between a satellite's expense, difficulty of replacement, and importance, versus the very basic requirements for certain attacks. A cyber attack requires only a trained person, a laptop and an uplink, and can be performed anywhere in the world. Jamming equipment is increasingly commercially available (with dual-use properties) and one does not have to jam the satellite itself, only its ground receivers. An even more interesting possibility is not the destruction of a satellite, but the subversion of its functioning to gain valuable information, or to feed false data to its operators. Moreover, the destruction or disruption of a satellite could be seen by the public as a victimless crime, which might serve various political agendas, as opposed to an actual violent terrorist attack.

Conclusions

Space systems are an emerging critical infrastructure, providing critical services to numerous and varied end-users and beneficiaries. They also possess a distinct risk profile, requiring a global framework if they are to be successfully managed. Any critical infrastructure system that depends on space systems must take into account these peculiarities - including the presence of specific threats - when assessing their own exposure to the risks of cascading disruptions. The critical energy infrastructure is one of these systems. It is undergoing a period of transition, in which critical dependencies on space systems have been established in certain subsectors of the larger system-of-systems, but many others can, conceivably, function well in the absence of space capabilities. Of course, this view ignores the complexity inherent in the numerous interdependencies between critical infrastructures in general, wherein exposure to critical space infrastructure disruption risk can also happen indirectly, via dependence on a third infrastructure system such as transport. Over time, the trend seems to be for access to space services to become more affordable, and for the services themselves to increase in quality. This is likely to increase the CEI dependence on CSI, especially since one of the main benefits of working with space systems is their potential for crisis and emergency situation management, which would mitigate some of the myriad risks, threats and vulnerabilities already affecting CEI.

⁵⁰⁶ Carmen Pardini, Luciano Anselmo, "Evolution of the Debris Cloud Generated by the FengYun-1C Fragmentation Event", Space Flight Dynamics Laboratory, *Istituto di Scienza e Tecnologie dell'Informazione „Alessandro Faedo”*, Pisa, Italy, 2007.

⁵⁰⁷ Austin Long, "Deterrence: From Cold War to Long War", Santa Monica, CA: Rand Corporation, 2008.

In order to emphasize the important connection between space and energy, we should mention the European Space Agency's Initiative for Space and Energy, which has foreseen the potential for space systems not just to act as an adjuvant to the CEI (monitoring operations, optimizing placement of renewables etc.), but also to contribute in other ways to innovation in the energy field. This includes, for instance, transfer of materials technology from the space sector (which has seen significant innovation in solar panel technology, energy conversion and new materials), as well as, in the long-term, extending the critical energy infrastructure into space, through space-born power sources.⁵⁰⁸ A series of specific proposals has also been formulated under this initiative for the short to medium term. These fit the critical infrastructure-specific vision of the Space-Energy dependence developed in this article:⁵⁰⁹

- Intelligent integrated grid monitoring, management and control;
- Intelligent planning, monitoring and diagnostic applications;
- Remote monitoring system for pipelines;
- Prediction of disruptive geomagnetically induced currents in networks;
- Small-scale power plant management and integration with electricity grid;
- Space infrastructure as enabling factor to increase the safety of nuclear energy production throughout the entire supply chain.

The potential for ESA's initiatives to create innovative solutions and promote the dissemination of good practices, rather than the ad hoc adoption of space capabilities in accordance with the financial means, sophistication and competitiveness of each energy actor or each national authority is a significant step towards addressing a new class of issues which threaten critical energy infrastructures – the complexity and uncertainty of trans-continental or regional critical energy infrastructures, where the security of the whole system is only as good as its weakest link, and where the reliance on national security actors and competent national authorities creates gaps in regional risk governance, allowing for the development of new vulnerabilities and threats.

Acknowledgement

The insights presented in this article were gleaned from a research project titled “Space Systems as Critical Infrastructure” led by the Romanian Space Agency, with the Military Equipment and Technologies Research Agency of the Romanian MoD, and the EURISC Foundation. The work was supported by a grant from the Romanian National Authority for Science Research, CNDI-UEFISCDI, project number 197/2012.

⁵⁰⁸ Carla Signorini, Isabella Duvaux-Bechon and Leopold Summerer, “Space and Energy - Current Status and Outlook”, 63rd *International Astronautical Congress*, Naples, 2012, <http://www.esa.int/gsp/ACT/doc/POW/ACT-RPR-NRG-1210-CB-IDB-LD-Space-and-Energy.pdf> (Accessed on 17.10.2015), p. 5.

⁵⁰⁹ Ibid, p. 6.

REFERENCES

- Airbus Defense and Space, "Space Resources for Stricken Japan",
<http://www.space-airbusds.com/en/news2/airbus-defence-and-space-satellites-observe-disaster-in-japan.html>, 2011.
- BUTT, Y., "The EMP Threat: Fact, Fiction and Response", Space Review, 2010.
- CAVELTY, M. D., PRIOR, T., "Resilience in Security Policy: Present and Future", "CSS Analysis in Security Policy", No. 142, Center for Security Studies, ETH Zurich, 2013.
- Committee on Earth Observation Satellites (CEOS), "Satellite Earth Observation for Disaster Risk Management", "CEOS Earth Observation Handbook 2012 - Special edition for Rio+20",
http://www.eohandbook.com/eohb2012/case_studies_satellite_earth_observation_for_disaster_risk.html, 2012.
- EASTON, I., "The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy", Project 2049 Institute,
http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf, 2009.
- European Commission, "Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure",
https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf, 2013.
- European Space Agency, "Free Access to Copernicus Satellite Data",
http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Free_access_to_Copernicus_Sentinel_satellite_data, 2013.
- European Space Agency website,
http://www.esa.int/Our_Activities/Navigation/Galileo_and_EGNOS
- GHEORGHE, A., BOUCHON, S. M., BIRCHMEIER, J., "Toward Guidelines for Regional Assessment of Vulnerability against Service Disruption of Critical Infrastructures", EsReDa, the 29th Seminar "System Analysis for a More Secure World" Proceedings, 2006.
- GHEORGHE, A., MASERA, M., WEIJNEN, M., DE VRIES, L., "Critical Infrastructures at Risk - Securing the European Electric Power Systems", Springer Netherlands, 2006.

GHEORGHE, A., SCHLÄPFER, M., "Critical Infrastructures: Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures", IRGC - ETH Document, Zürich, 2004.

GORDON, K., DION, M., "Protection of Critical Infrastructure and the Role of Investment Policies Relating to National Security", Investment Division of the Directorate for Financial and Enterprise Affairs, Organisation for Economic Co-operation and Development, 2008.

GUPTA, V., PABIAN, F., "Viewpoint: Commercial Satellite Imagery and the CTBT Verification Process", "The Nonproliferation Review", Vol. 5, Issue 3, 1998.

HAEME, T., "Use of Satellite and Airborne Remote Sensing in the Safeguards of a Nuclear Waste Repository Site", "Safeguards for Final Disposal of Spent Nuclear Fuel - Methods and technologies for the Olkiluoto site", Olli Okko (ed.), 2003.

HAPGOOD, M., THOMSON, A., "Space Weather, Its impact on Earth and Implications for Business", Lloyd's 360 Risk Insight Briefing, 2010.

HOKSTAD, P., UTNE, I., VATN, J., "Risk and Interdependencies in Critical Infrastructures", Springer Series in Reliability Engineering, Springer, Trondheim, Norway, 2012.

IWASA, T., "Disaster Monitoring Activities in Japan",
<http://www.unoosa.org/pdf/pres/stsc2012/tech-11E.pdf>, 2012.

KELSO, T. S., "Iridium 33/Cosmos 2251 Collision", Center for Space Standards and Innovation, Colorado Springs, USA, 2009.

KLOTZ, W., et al., "Guiding Principles for the Nation's Critical Infrastructures", American Society of Civil Engineers, 2009.

LONG, A., "Deterrence: From Cold War to Long War", Santa Monica, CA, Rand Corporation, 2008.

National Research Council, "Severe Space Weather Events: Understanding their Economic and Societal Impact", Workshop Report, Washington DC,
<http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf>, 2008.

PARDINI, C., ANSELMO, L., "Evolution of the Debris Cloud Generated by the FengYun-1C Fragmentation Event", Space Flight Dynamics Laboratory, Istituto di Scienza e Tecnologie dell'Informazione", Pisa, Italy, 2007.

Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization, "Overview of the Verification Regime",

<http://www.ctbto.org/verification-regime/background/overview-of-the-verification-regime/>

RINALDI, S., PEERENBOOM, J., KELLY, T., "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine*, Vol. 21, Issue 6, 2001.

Royal Academy of Engineering, "Extreme Space Weather: Impacts on Engineered Systems and Infrastructure", London, 2013.

SIGNORINI, C., DUVAUX-BECHON I., SUMMERER L., "Space and Energy - Current Status and Outlook", *63rd International Astronautical Congress*, Naples, <http://www.esa.int/gsp/ACT/doc/POW/ACT-RPR-NRG-1210-CB-IDB-LD-Space-and-Energy.pdf>, 2012.

Sr. Capt. Bart Smedts, "Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future", Focus Paper 15, *Center for Security and Defence Studies*, Royal High Institute for Defense, 2010.

"Space: Dependencies, Vulnerabilities and Threats", Section 4-8, Centre for Developments, Concepts and Doctrine, Ministry of Defense, United Kingdom, 2012.

Space Weather Scales, NOAA Space Weather Prediction Center,
http://www.swpc.noaa.gov/NOAA_scales/

Tauri Group, "2015 State of the Satellite Industry Report", commissioned by Satellite Industry Association, <http://www.sia.org/wp-content/uploads/2015/06/Mktg15-SSIR-2015-FINAL-Compressed.pdf>, 2015.

Union of Concerned Scientists, Open-Source Satellite Database Statistics,
<http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.Vg0BUCvkVTB>

VUGRIN, E., WARREN, D., EHLEN, M., "A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane", Sandia National Laboratories, *6th Global Congress on Process Safety*, 2010.

WEAVER M. et al., "Halloween Space Weather Storms of 2003", NOAA Technical Memorandum OAR SEC -88, NOAA, 2004.

WEEDEN, B., "Billiards in Space", *Space Review*,
<http://www.thespacereview.com/article/1314/1>, 2009.

YOSHIMOTO, S. et al., "Environment Monitoring of Fukushima and Chernobyl Areas using a Constellation of Earth Observation Microsatellites (Japan-Ukraine

Cooperation Technical Demonstration Program for Supporting Aftermath Responses to Accidents at Nuclear Power Stations)", *5th Nanosat International Symposium NSS-05-0104*, 2013.

THREAT INTELLIGENCE FOR CIP

Oscar SERRANO

ABSTRACT

Across the world, organizations have teams gathering threat data to protect themselves from incoming cyber attacks and to maintain a strong cyber security posture. Teams are also sharing information, because along with the data collected internally, organizations need external information to have a comprehensive view of the threat landscape. Industry is not indifferent to this requirement, and several commercial companies are starting to offer solutions in the areas of information sharing and threat management. This paper summarizes the main concepts that policy and industry professionals should be aware of when drafting an organizational cyber information sharing strategy.

Key Words: Cyber Security; Data Sharing; Threat Intelligence Management; NATO; TAXII

Introduction

Ensuring the cyber security of critical infrastructures is a daunting task, which starts with defining the scope. Although the general idea is easy to understand, the reality is that there is no consensus on the most basic terms. In general, each nation or international organization has a different understanding of what is meant by critical infrastructure, a cyber attack or the difference between a cyber attack and an act of force (as defined by the UN charter). Based on US definitions, critical infrastructures, as defined by the 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), are:

“Systems and assets, whether physical or virtual, that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

Based on this definition, US Presidential Policy Directive 21 identifies 16 critical infrastructure sectors:

- Chemical
- Commercial facilities
- Communications

- Critical manufacturing
- Dams
- Defense industrial bases
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and public health
- IT
- Nuclear reactors
- Transportation
- Waste and wastewater systems

To varying degrees, all these sectors rely on IT systems for their operations and this makes them prone to cyber attacks. However, there are different levels of awareness across the sectors in regard to the risk posed by cyber attacks. For example, financial services are by far the most advanced with respect to cyber security and fraud detection, mainly because they have a greater risk of direct financial compromise; the healthcare sector is primarily concerned about privacy and compliance issues, while for the industrial sector the concept of cyber security is relatively new. Until recently, the supervisory control and data acquisition (SCADA) systems that were used in many industrial processes were thought to be too complex to be targeted by opportunistic attackers, and the notions of Advance Persistent Threats (APT) and nation-sponsored attacks were still not seen as realistic threat scenarios. Moreover, SCADA systems normally run in isolated networks, with no internet connectivity, and that isolation was, naively, thought to provide adequate security. Now, it is well known that SCADA systems are the target of state-sponsored cyber attacks, and that isolated networks and air gaps are not going to stop determined intruders.

During recent years, there has been a growing interest in cyber security in general and of critical infrastructures in particular. For example, the 1999 NATO Strategic Concept emphasized the concerns of the Allied Nations regarding critical infrastructures: “*Alliance security can be affected by [...] the disruption of the flow of vital resources.*” Similarly, in 2010 the Strategic Concept affirmed NATO’s commitment to “*develop the capacity to contribute to energy security, including protection of critical infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning*”. However, it was not until 2010 that the Strategic Concept explicitly identified the risk posed to the Alliance by cyber attacks: “*Cyber attacks are becoming more frequent, more organized and more costly in the damage that they inflict on [...] transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability.*”

In view of the wide array of sectors that can be considered to be critical, ensuring cyber security of these systems entails a range of activities. The NATO Communications and Information Systems Security Capability Breakdown,⁵¹⁰ identifies five areas of improvement (Prevent, Defend, Assess, Sustain and Inform), and for each of them it defines the high-level activities that can be applied to, *inter alia*, critical infrastructures:

Table 1. NCI Agency Security Capability Breakdown

Prevent	CIS protection	Data protection	Identity and access management	Asset configuration management	and
Defend	Monitor	Detect	Respond	Recover	
Assess	Manage risk	Manage trust	Assess security	CIS Audit	
Sustain	Govern	Design and implement	Educate, train and exercise	Improve	
Inform	Organize	Collect	Analyze	Report and share	

All these activities are relevant to the protection of critical infrastructures. However, this chapter focuses exclusively on the “Inform” branch, covering the information-sharing aspects of cyber-securing critical infrastructures.

Threat Intelligence

Current commercial cyber security technology for detection of cyber attacks is based mainly on signatures. Although there has been a great deal of research into behavior-based systems, these systems have to date failed to provide consistent detection capabilities.⁵¹¹ This implies that with current technologies there is no detection capability against exploits using zero-day vulnerabilities; however, known attacks can be detected with a certain level of assurance. Regardless of the level of assurance that signature-based systems can provide, attackers are successfully reusing exploits and this is because old exploits still work. For example, open source tools such as Metasploit provide a repository of exploits targeting well-known vulnerabilities. Although patches have been released for most of the vulnerabilities targeted by Metasploit, the framework is still the best known tool for the generation of opportunistic malicious code. The reason that attackers can successfully reuse exploits is that most

⁵¹⁰ Geir Hallingstad and Luc Dandurand, “CIS Security (Including Cyber Defense) Capability Breakdown”, *NATO Consultation, Command and Control Agency Reference Document RD-3060*, The Hague, Netherlands, Technical Report, November, 2011.

⁵¹¹ Robin Sommer and Vern Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” in *Security and Privacy (SP), 2010 IEEE Symposium*, 2010, pp. 305–316.

users are not aware of the vulnerabilities or the risk that they take by failing to apply regular patching strategies. The lack of regular patching is amplified in out-of-line systems (such as industrial control systems) because the updates to these systems require manual downloads and application.

In this context, the flow of cyber information is of paramount importance. Because of the lack of information sharing, attackers need to work on an exploit only once and can reuse it on multiple targets, while each defender is forced to work individually on detecting and analyzing each attack. No organization has sufficient resources and knowledge to perform this work independently. The information that can be exchanged between organizations to support the collective burden of detecting and analyzing cyber threats is known as *threat intelligence*. Cyber threat intelligence can be obtained internally or from external sources, and is defined by Gartner as:

“Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”

The generation of threat intelligence is a labor intensive task, and many organizations are willing to collaborate on this. However, current practices and information systems have until now provided limited support for effective and efficient collaboration. Thus even though organizations may be ready to participate in burden-sharing approaches, in many cases the associated level of effort required in the absence of a facilitating system is simply too high. This is why recently there have been significant efforts towards the development of new cyber security information-sharing capabilities. Although the existing solutions are still not problem-free, they allow organizations to share information effectively. A review of the pending issues and the possible solutions is presented in⁵¹². In the remainder of this chapter the discussion concentrates on the current existing solutions and how they can provide value to the critical infrastructure sector, even though there is still room for improvement.

⁵¹² Oscar Serrano, Luc Dandurand, and Sarah Brown, “On the Design of a Cyber Security Data Sharing System”, *Proceedings of the 2014 ACM Workshop on Information Sharing and Collaborative Security*, New York, USA, 2014, pp. 61–69.

Standards

There is no definition of which data constitutes threat intelligence and which does not. It is generally accepted that in order to defend communication and information systems efficiently, the following information is required:

Table 2. Threat Intelligence Sources

Vulnerability information	Threats	Events information	Best practices
Affected systems	Names/pseudonyms of actors	Victim demographics	Security guidance
Effects (known exploits)	Countries of origin	Involved actors	Secure coding practices
Patches and mitigations	Attack patterns	Affected assets (software and hardware)	Security configurations
Vulnerability assessment tests/results	Events and incidents	Actions performed (e.g. malware, protocol specifications)	
	Signatures and indicators of compromise	Impact (in terms of confidentiality, integrity or availability)	
	Black or white list information (IP addresses)	Discovery and response information	

The requirements for sharing these types of information have long been identified and there are a number of standards and frameworks that enable the structured exchange of this information. Organizations in the critical infrastructure sector willing to share cyber information should take advantage of these existing standards and use those that best suit the requirements of their community. The current most important standards are described below.

1. Security Content Automation Protocol (SCAP)

The Security Content Automation Protocol (SCAP) is a set of interoperable specifications that are extensively used by the community and are made use of by other standards. The specifications include:

- Enumerations of vulnerabilities, platforms and configurations:
 - Common Vulnerabilities and Exposures (CVE)
 - Common Platform Enumeration (CPE)
 - Common Configuration Enumeration (CCE)
- A common way to express measurements:
 - Common Vulnerability Scoring System (CVSS)
- Policy compliance:
 - eXtensible Configuration Checklist Description Format (XCCDF)
- Assessing systems for known vulnerabilities:
 - Open Vulnerability and Assessment Language (OVAL).

This information is freely accessible via the National Vulnerability Database, which offers the data in human-readable format via a website, as well as in machine-readable format using predefined XML schemas. The information can also be obtained via RSS data feeds. SCAP specifications provide the basic enumerations on which other cyber security standards rely.

2. Incident Object Description Exchange Format (IODEF)

IODEF provides an XML schema for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRT) about computer security incidents. An IODEF document can represent one or more incidents, each of them containing the XML classes that encode information, such as the incident tracking numbers of related incidents, timestamps (first detection of the incident, start time, end time, report time), free-form textual description of the incident, characterization of the impact, the techniques used by the intruder, contact information for the parties involved, description of the events and the log of significant events or actions that occurred during the course of handling the incident.

The information, encoded as XML classes, is expressed using attributes and enumerations defined in the standard. This facilitates the automatic exchange of information. To provide some flexibility, each incident can be extended by using the Additional Data class, which can be used to exchange information that does not fit the classes and enumerations defined in the standard. Although IODEF is an important standard to consider it will most likely be superseded by STIX in the near future.

For more information about IODEF, the Internet Engineering Task Force (IETF) in RFCs 5070 and 6685 provides a complete definition of the standard.

3. Open Indicators of Compromise (OpenIOC)

OpenIOC is maintained by Mandiant and used mainly by its products, though it has also been released as an open standard. OpenIOC defines a number of terms that can be used to define indicators of compromise. The enumeration covers, for example,

terms such as *File Extension*, *File MD5* and *registry path*. Several of these terms can be combined into an IOC document to define a malware sample. An OpenIOC XML document in the latest version (1.1) contains three main sections:

- Metadata: Header containing metadata about the entire Indicator.
- Definition: A Boolean logical evaluation that determines whether or not the indicator is triggered.
- Parameters: Assignable metadata that can be applied to any element in the criteria section of the IOC.

OpenIOC is best suited for the exchange of IOCs that can be automatically imported into automatic tools such as vulnerability scanning tools.

4. VERIS Framework

The Vocabulary for Event Recording and Incident Sharing is maintained by VERIZON, which uses it to release its annual Data Breach Investigation Report.

The VERIS Framework is organized in the following five sections:

- Incident Tracking
- Victim Demographics
- Incident Description
- Discovery & Response
- Impact Assessment.

The most important section is the incident description, which is described by means of the *four A*: *Actors*, *Actions*, *Assets* and *Attributes*. VERIS provides the data schemas and the enumerations needed to complete all the sections. The schemas can be implemented using any data modeling technology (e.g. XML, JSON or referential data models). The framework is aimed at high-level reporting of incidents and is most suitable for the generation of strategic data such as management dashboards.

5. Cyber Security Information Exchange Framework (x.1500 Cybex)

The Cybersecurity Information Exchange Framework is an ITU-T standard that due to its complexity has not gained widespread acceptance. The goal of CYBEX was to enable language-agnostic information sharing. For this purpose, CYBEX defines a container in which information in other standards can be encapsulated. A CYBEX document consists of five major building blocks:

- Information description block: Defines the encoding format of the information using standards such as CVE, CAPEC or OVAL.
- Information discovery block: Identifies the location from which the information can be queried.

- Information query block: Defines the method for requesting the information from the owner.
- Information validation block: Checks if the information and the sender can be trusted.
- Information transport block: Defines the protocols required to transmit the information over the network.

CYBEX links these five blocks to describe information, identify the organization that owns the information, send queries to them, and ensure the identity of the organization in order to realize the information exchange.

6. MITRE Standards

a) *Cyber Observable eXpression (CybOX)*

CybOX is a standardized language for the definition of measurable events or stateful properties that are observable in a given operational domain. Examples of cyber observables include registry key creation, file deletion, HTTP GET requests, the MD5 hash of a file, the value of a registry key, and the name of a process. These observables are similar to those that can be defined with the OpenIOC. CybOX is the basic building block that is made use of in other MITRE standards such as STIX.

b) *Malware Attribute Enumeration and Characterization (MAEC)*

MAEC is a standardized language for sharing XML-encoded structured information about malware, based on attributes such as behaviors, artifacts, and attack patterns. MAEC is used to describe malware from the very basic technical level up to the more abstract contextual levels of behaviors and capabilities. MAEC is structured to embed CybOX content, such that MAEC is used to define the behaviors and capabilities of the malware, while CybOX describes the low-level information about the indicators of compromise.

MAEC provides three different levels of schemas:

- MAEC Bundle: the MAEC Bundle data model provides the ability to capture and share data obtained from the analysis of a single malware instance. At this schema level the actions, behaviors and capabilities of the malware are defined.
- MAEC Package: the same malware instance and its variants can be analyzed using different tools, and each of these analyses creates a separate MAEC Bundle. The collection of MAEC Bundles can be shared as part of a MAEC Package.
- MAEC Container: the MAEC container allows encapsulation of a collection of MAEC Packages for sharing.

MAEC defines default vocabularies (collections of enumerated terms) that can be used to enable sharing machine-readable data. For example, if the action *download file* needs to be specified, this can be done using the vocabulary

NetworkActionNameVocab-1.0, which contains the term *download file*. It is possible to extend the default vocabularies as well as to use non-standard vocabularies if required.

c) Common Attack Pattern Enumeration and Classification (CAPEC)

CAPEC provides the means to describe attack patterns such as those executed, for example, during SQL injections or cache poisoning attacks. A CAPEC record consists mainly of the attributes listed in Table 3:

Table 3. Attributes Contained in a CAPEC Record

Identifying Information	Related Vulnerabilities	Scoping and Delimiting Information
Attack Pattern ID	Method of Attack	Severity
Attack Pattern Name	Examples-Instances	Likelihood of Exploit
Describing Information	References	Attack Prerequisites
Description	Prescribing Information	Attacker Skill or Knowledge Required
Related Weaknesses	Solutions and Mitigations	Resources Required
Attack Consequence	Motivation-	Context Description

Most of the attributes are free text entries, but CAPEC provides some enumerated lists for entries such as *Method of Attack* or *Attack Motivation-Consequence*.

d) STIX (Structured Threat Information eXpression)

STIX is the latest standardized language for the representation of cyber threat information, and during its short life to date has gained major support and widespread adoption by the cyber security community. STIX is originally represented using XML, however it could also be implemented using any other data structure such as JSON, RDF/OWL or protocol buffers. It is based on eight core classes:

- Observable: Cyber Observables represented using CybOX. These are the basic STIX elements.
- TTP: Adversary Tactics, Techniques, and Procedures represent an adversary's specific behavior, including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc. Some portions of this structure are generated using MAEC or CAPEC.
- Indicator: One or more Observable patterns bundled into a class providing details such as confidence, impact, time windows or source of the indicator. Indicators are potentially mapped to one or more TTPs, Campaigns and Courses of Action.

- Incident: A discrete instance of one or more indicators affecting a particular organization. The Incident is also used to represent unconfirmed events as well as analysis activities. The most important incident information consists of: victim, reporter of the incident, times (of compromise, detection, restoration and reporting) and affected assets. In addition, an incident may include other information such as impact assessment, intended effects, nature of compromise, confidence, handling guidance or log of actions taken. An incident is related to one or more Indicators, TTPs, Threat Actors and Courses of Action.
- Exploit Target: Vulnerabilities or weaknesses in software, systems, networks or configurations that are targeted for exploitation by the TTP of a Threat Actor. STIX makes use of existing standards such as Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE) or Common Configuration Enumeration (CCE) identifiers to construct this class.
- Course of Action: Contains a structured description of the measures taken to address the threat, including information such as the Course of Actions type, description, objective, structured representation, likely impact, likely cost, estimated efficacy or handling guidance. Each course of action can be potential, recommended, requested or taken for a previously defined incident or campaign.
- Threat Actor: Cyber Threat Actors are characterized by their identity, suspected motivation and suspected intended effect. Each Threat Actor is related to other Threat Actors (associated) as well as to historical data about TTPs and Campaigns.
- Campaign: Cyber Attack Campaigns are instances of a Threat Actor pursuing an intent. Campaigns are defined by attributes such as confidence in the assertion, source of the information and handling guidance. A campaign is attributed to at least one Threat Actor and has one or more related incidents, campaigns and TTPs.

Almost everything in STIX is optional, enabling users to make use of only the portions of STIX relevant for their use case or community. Existing standardized languages are used as optional extensions where appropriate. For example, in certain cases, it can be useful to include a full representation of malware behavior in order to share it with other parties, or to relate its behavior to other pieces of intelligence in STIX. This malware behavior is modeled in STIX by using MAEC. STIX directly generates CybOX and provides a mechanism to embed other standards such as MAEC, CAPEC and CVE.

e) **TAXII (Trusted Automated eXchange of Indicator Information)**

TAXII is a lightweight XML-over-HTTPS transport protocol that standardizes how STIX data can be exchanged across organizational boundaries. TAXII exchanges data collections, which are organized sets of data as defined by the producer. As a pure transport protocol TAXII does not define mechanisms outside the scope of transport

itself. Thus, important aspects of information sharing such as the creation of trust relations or the management of authentication and authorization mechanisms are not defined by TAXII. If required, they need to be implemented independently of the TAXII specification. TAXII can be used to implement three different data sharing models: peer-to-peer, publish-subscribe or spoke-hub, depending on the needs of each organization. To enable these models TAXII defines four optional services:

- Discovery: To query the services supported by a TAXII server
- Collection Management: To obtain the list of all data collections in the server and to manage subscriptions in a publish-subscribe model.
- Inbox: To implement a push mechanism
- Outbox: To implement a pull mechanism

Each organization can implement TAXII servers and clients using only the services that they require. TAXII messages can also include queries that are used to provide characteristics against which content records are compared. TAXII provides a query format specification, used to define query expressions allowing requestors to collect only content that meets these criteria.

Collaborative Data Sharing Solutions

Most cyber security companies have their own unit dedicated to providing threat analysis feeds and reports to their subscribers. Some of the best known are DeepSight (Symantec), Wildfire (Palo Alto), Global Threat Intelligence (McAfee), Reputation Security Monitor (ArcSight), X-Force (IBM), Talos (CISCO) and ThreatCloud (CheckPoint). The number of sources and amount of data is so overwhelming that a new concept called *Threat Intelligence Management Platform* has been coined. The aim of a Threat Intelligence Management Platform would be to manage cyber threat intelligence feeds and convert them into actionable information that can be delivered to the different tools and stakeholder. For example, the platform would receive data feeds into STIX, normalize, enrich and link them with other data received from other sources and finally convert them into rules that can be automatically pushed to SIEMs, NIPs or other security products.

Threat intelligence services are highly valued, and many organizations are interested in obtaining data or data management services from commercial providers. However, others are interested in sharing data inside their communities using freely accessible tools that enable burden sharing. This section lists some of the tools that are currently being used by different communities to share cyber security information, as well as some of the sectors of cyber security communities that are relevant to the protection of critical infrastructures.

1. Malware Information Sharing Platform (MISP)

MISP is a freely available platform that is actively being improved. It is aimed at the sharing and storing of Indicators of Compromise of targeted attacks. MISP stores data

using its own internal data model and allows exporting of data into Snort/Suricata IDS rules, STIX, OpenIOC, plain text or comma-separated values (csv) exports. Importing data can be done using free-text import, OpenIOC, batch import, or using the preconfigured or custom templates. MISP is currently in use by many national and international CERT groups (including the NATO Computer Incident Response Capability) as well as by ISAC groups and private companies. MISP does not support TAXII, so its use is restricted to the MISP community, and currently it offers no support for storing some of the threat intelligence information defined in STIX such as campaigns, threat actors and TTPs. However, MISP is actively being developed by a community of CERT groups and these features are foreseen for future versions.

2. Collaborative Research into Threats (CRITS)

CRITS is a free open-source solution developed by MITRE for the sharing of threat intelligence. It implements MITRE standards such as STIX and TAXII. CRITS was developed in 2010 as an internal tool for MITRE use, and is still being improved. It can be installed locally for use as a threat repository in a private isolated instance, or as a TAXII server sharing information with other trusted organizations.

3. Microsoft Interflow

Interflow is Microsoft's answer to the problem of sharing cyber security and threat information. It provides a distributed exchange platform for the storage and exchange of data feeds using STIX and TAXII. Its goal is to facilitate security automation by providing machine-readable data automatically. It allows users to create their own sharing communities, and to define what to share and with whom. Interflow runs on Microsoft Azure public cloud and provides an open SDK aimed at enabling automation. Microsoft envisions the creation of plug-ins to the most used security appliances using this SDK.

4. IBM X-Force Exchange

IBM X-Force is the newest tool on the list, and is currently under active development by IBM's threat intelligence group. It is a threat intelligence sharing platform that runs in the IBM cloud, providing 'collections' for users to search, store and share aggregated information. One of the objectives of IBM X-Force is to facilitate burden-sharing collaboration and/or outsourcing for the generation, refinement and vetting of cyber security data. X-Force Exchange integrates out of the box with the IBM security products suite and in particular with the QRadar Security Intelligence Platform, providing it with real-time data from the IBM X-Force security analysis team enriched with data collectively generated from the community. At the moment, IBM X-Force Exchange is a free SaaS (software as a service). As for all recent tools, IBM X-Force supports STIX and TAXII for the exchange of cyber information.

5. Soltra Edge

Soltra is a joint venture between the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Depository Trust & Clearing Corporation (DTCC).

Soltra maintains an open and interoperable system for the exchange of cyber threat intelligence using TAXII and STIX. The system, named the Soltra Edge server, contains a STIX information repository, a TAXII server, and a web interface. The Soltra Edge server mitigates the complexity of STIX and TAXII for the end users by providing a ready-to-deploy TAXII server implementing access controls and trust groups. Soltra was previously known as Avalanche.

Communities

Many organizations have inter-sectoral data sharing agreements; this section describes the ISAC community because it is important to the critical infrastructure sector and the Cyber Threat Alliance, which is one of the newest communities of major cyber security organizations.

1. Information Sharing and Analysis Centers

A number of critical infrastructure organizations have established a sufficient degree of mutual trust to enable collaboration. These partnerships are given a framework in the Information Sharing and Analysis Centers (ISAC). ISAC encompasses trusted entities, some of which are world-wide and some of which are restricted to the USA, which provide comprehensive sector analysis that is shared within the sector, with other sectors, and with governmental organizations. Some of the most important ISAC communities are:

- A-ISAC: The Aviation Information Sharing and Analysis Center (A-ISAC) provides an aviation-focused information sharing and analysis to help protect aviation businesses, operations, and services globally. Membership is open to trusted private sector companies engaged in international aviation.
- DIB-ISAC: The Defense Industrial Base ISAC provides their members with a broad, multi-sector view of emerging threats, sharing information on and analysis of security issues related to cyber and physical events, threats and intrusions. Its aim is to facilitate the sharing of best practices in security, and enhance the ability of the DIB sector to prepare for, respond to and mitigate risk due to security threats, vulnerabilities and incidents.
- DNG-ISAC: The Downstream Natural Gas ISAC serves natural gas utility (distribution) companies by facilitating communications between participants, the federal government, and other critical infrastructures. Specifically, the DNG-ISAC coordinates very closely with the ES (Electric Sector) ISAC and shares information between electric, combination (natural gas and electric) and natural gas utilities.
- EMR-ISAC: The Emergency Services ISAC collects and analyzes critical infrastructure protection and resilience information of potential relevance for the sector.

- ES-ISAC: The Electricity Sector ISAC establishes situational awareness, incident management, coordination and communication capabilities within the sector through timely, reliable and secure information exchanges.
- FS-ISAC: The Financial Service ISAC shares information between financial services firms worldwide. It constantly gathers information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources to disseminate physical and cyber threat alerts. FS-ISAC is one of the most active information sharing groups and has recently started using STIX.
- ISC-ISAC: The Industrial Control Systems ISAC helps facilities develop situational awareness in support of local, national and international security. The ICS-ISAC maintains a Soltra Edge server for real-time information sharing. ICS-ISAC members have access to this server through peer-to-peer TAXII feeds (or through a website).
- NH-ISAC: The National Health ISAC serves to protect the US healthcare and public health critical infrastructure against security threats and vulnerabilities.
- ONG-ISAC: The Oil and Natural Gas ISAC is the central platform for cyber threat information for the oil and natural gas industry. It protects the industry's exploration and production, transportation, refining, and delivery systems from cyber attacks through analysis and sharing of timely and trusted cyber intelligence.

2. Cyber Threat Alliance

Although participation in the Cyber Threat Alliance is open, in practice it is composed of major cyber security vendors and is not intended for organizations in other sectors. The alliance was founded by Fortinet, Intel Security, Palo Alto Networks and Symantec for the purpose of sharing threat information. The alliance provides actionable threat intelligence from contributing members, including information on zero-day vulnerabilities, botnet command and control (C&C) server information, mobile threats, and indicators of compromise (IOC) related to advanced persistent threats (APT), as well as providing commonly shared malware samples. The alliance is committed to using standards such as STIX and TAXII.

3. The Way Forward

Exchange of cyber threat information is rapidly developing, and organizations can now take advantage of the standardization efforts that have taken place in the last decade. STIX and TAXII are the current *de facto* standards for cyber information exchange and organizations in the critical infrastructure sectors should begin adopting them. The easiest approach to cyber threat intelligence sharing is to join already existing communities and to adopt existing tools. In some cases, this may require the deployment of organizational TAXII servers or clients, and in that case OpenTAXII, YETI and Soltra Edge Server are the current available solutions. Similarly

organizations looking to develop their own internal databases may want to use schemas based on STIX, as it enables the exchange of information without costly data mapping processes.

Sharing cyber information is necessary but not in itself enough for an organization to maintain a comprehensive cyber threat picture. The solutions presented in this chapter can address the most acute requirements regarding sharing cyber threat information, but in reality organizations starting to collect threat intelligence will soon notice that they are in the need of tools to support the generation, refinement, and vetting of the large quantities of data that they will receive. Depending on the maturity of an organization, intelligence is used either as a direct input to existing business capabilities or as a business capability in itself (“cyber intelligence practice”). When used as direct input to existing capabilities, the intelligence is used as an actionable information element. In more mature organizations, the intelligence practice is the process by which intelligence strategy, budget, process, competency and objectives are anchored in the organization and made predictable and accountable to the security organization. Most large enterprises with substantial security programs have or are building a cyber intelligence practice. Critical infrastructure organizations should, in the longer term, aim to establish cyber intelligence practices. The requirements of a cyber intelligence practice go further than the sharing of threat intelligence, and require processes to collect information from a wide variety of sources, to manage the flow of information and to convert it into knowledge and actions. Among the challenges that still need to be addressed are those related to:

- Normalization and consolidation: Managing data from a wide range of sources requires the capability to link similar pieces of information, and merge information to reduce to the best fit or de-conflict different views of the same events.
- Enrichment: Integrating any number of data elements from external sources with the information collected in a threat intelligence platform to enhance the data with contextual data to support a better analysis.
- Quality determination: Including determination of quality attributes such as data relevance, timeliness, accuracy, precision and consistency.
- Complex analysis: Capability to infer intelligence based on indirect relationships; inference based on not only content, but also on relationships and potential sameness and/or overlap with other pieces of intelligence.
- Delivery: The capability to deliver the intelligence to the intended users. High-level executives are interested in the threat landscape and trends, while a threat analysis team will be interested in various indicators of compromise.
- Analytic management and collaboration: In order to allow organizations to pool resources towards common goals.
- Integration: Availability of open APIs to manage the integration with technical tools.

Industry is not indifferent to these requirements and the difference between content aggregation and threat intelligence management is quickly disappearing as organizations are increasing aware of the need to manage threat intelligence. Several commercial companies (e.g. Intelworks, Soltra, Threatstream, ThreatConnect, Vorstack, ThreatQuotient, Microsoft Interflow and Comilion Exchange) are developing or upgrading their products to address the challenges listed above. In the near future these products will be available to the CIP sector and companies will be able to extract maximum value out of collected intelligence, and translate those findings into action for a broad range of stakeholders.

REFERENCES

HALLINGSTAD G., and DANDURAND L., "CIS Security (Including Cyber Defense) Capability Breakdown", NATO Consultation, Command and Control Agency Reference Document RD-3060, The Hague, Netherlands, Technical Report, November 2011.

SOMMER R., and PAXSON V., "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection", *Security and Privacy (SP), 2010 IEEE Symposium*, 2010.

SERRANO, O., DANDURAND, L., and BROWN, S., "On the Design of a Cyber Security Data Sharing System", *Proceedings of the 2014 ACM Workshop on Information Sharing and Collaborative Security*, New York, USA, 2014.

UNDERSTANDING NATO'S NEW CIP POLICIES: COMMON EFFORTS AND SOLIDARITY

Prof. Dr. Mesut Hakkı CAŞIN

ABSTRACT

Traditional national security policy objectives of modern states depend on the integrity of a nation's borders and institutions. However, at the first quarter of the 21st century, security environment was radically transformed either by states or individual attacks to critical national infrastructures by using tactics of computerized high-technology crimes including cyber attacks. Today, international community comes face to face with the growing potential of security threats, but its results, size and hazardous negative impacts are difficult to predict.

In this picture, a recent development about energy security involves more important initiatives for NATO's new priorities that have been set for dealing with potential threats on the agenda. Critical infrastructure protection-CIP has been identified to examine what its potential roles might be under a major dominant factor in international security spheres in the past, today and in the future. In spite of complex difficulties of CIP, NATO challenges to find reasonable security and deterrence solutions together by all common efforts and capabilities between the allies with the solidarity mentality.

Key Words: NATO, CIP, Cyber Defense, Collective Security, Energy Security

Introduction

“Energy security is not a call to arms. But when it comes to understanding the security implications of global resource developments, NATO must be ahead of the curve.”

Former NATO Secretary General Anders Fogh Rasmussen

We have ongoing critical debates about common energy security roles in particular, concerning cross-border and international threats as well as information sharing and new mission mandate waiting for NATO Alliance. Why is there a need for real change and improvement in NATO CIP positions? How can NATO develop innovative and useful ways to address these challenges? Does the Alliance need to change its way of carrying out defense missions? What kind of impacts do new energy security threats and challenges have on the future of the Organization? In order to find academic

answers to these questions, first we have to be familiar with the ongoing political environment and correctly define preventive capabilities of NATO which has been regarded as the most reliable transatlantic forum for developing and refining hazardous response capabilities against the attacks to operating energy network systems. In this article, we will briefly explain NATO CIP initiatives and efforts of allies.

The Changing Nature of Traditional Energy Security and the Potential Role of NATO

For all states and NATO, energy is one of the most basic crucial elements of sustainability in modern societies. As summarized above, contemporary way of life is strongly connected to critical energy infrastructures-CIP such as oil and gas pipelines, nuclear and conventional power plants, maritime and railroad transport, harbors, industrial electricity distribution, and IT networks as well as military-economic facilities. Regarding NATO member states' dependence on external fossil energy resources, any serious failure in these vital energy security services or any break down in the essential elements of infrastructure will have negative consequences which could spread to other economic sectors as well because of interdependencies.

However, today or in the middle term, it is possible to come face to face with unpredictable serious damages. Thus, after the Cold War and ongoing Russia-Ukraine tension in the Black Sea region, CIP policies based on possible energy supply security threats are particularly salient for the changing nature of NATO's security strategies. In this regard, we intend to provide an essential framework that encourages the formulation and implementation of appropriate policies and institutional management of CIP security that is related to NATO and Transatlantic community. It is about the preparedness of national and private business infrastructure, overall infrastructure resilience and energy reliability. Indeed, NATO provides a platform for intelligence-sharing, training and education, and the exchange of best practices on the protection of critical energy infrastructure with partner countries, other institutions, and the private sector. Therefore, NATO's role could be to express its political will through its member states, to actively counter these emerging security challenges, to put forward large demonstration projects, and to make valuable and practicable contribution.

For allies, expectations to be realized in the future with the aim of maintaining its credibility as a security organization addressing current international security threats effectively, NATO was called upon to expand its non-military capabilities and deepen its relations with its partner nations. NATO's conceptualizing in CIP started in the post-Cold War era and has been progressively consolidated in Riga, Bucharest, Lisbon, and Chicago summits. Recently, all NATO members think that CIP primarily has a dual face both national and common responsibility between the partners. The transatlantic energy dialogue, energy challenges, and outlining the discrepancy between the volume of energy produced and/or imported-consumed is based on the new security policy balance which changes common issues such as collective energy security,

energy efficiency and alternative energy sources.⁵¹³ Euro-Atlantic states represent the world's largest energy market. NATO countries produce approximately 23% of the world's energy; however, they consume almost 40% of the world's supply. Main alarming situation has emerged just after the oil embargo applied by OPEC countries in early 1970s. After the Israel-Arab wars, Western Block countries decided to shift energy supply alternatives from the Middle East to USSR and other African countries as potential energy suppliers.

Most importantly, there was a fundamental concern about creating energy security guarantees without breakout risks, such as September 11 terrorist attacks and 2006 Russia-Ukraine gas crisis, 2008 Russia-Georgia war and recently Crimea tensions indicate the reflected new security threats and uncertainties around the surrounding global energy supply. Thus new energy environment policies are needed for the protection of vital transit routes on the Middle East and Eurasia axis, and energy security issues are likely to gain importance.⁵¹⁴ According to the global energy system, nearly 80% of the world's hydrocarbon reserves are now under state control. However, Middle East, Central Asia and North Africa as energy supply regions consist of politically unstable countries, a situation that creates 'new worries for the marketing countries'. Secondly, the global energy system is being transformed by concerns about climate change. Hydrocarbon combustion emits greenhouse gases and thereby causes global warming and other measurable changes in the earth's climate. Thirdly, increasing attacks of non-state actors and cyber war threats against critical energy infrastructures have triggered cooperation with its transatlantic partners. For NATO, supply guarantee and CIP are the main aspects of the energy security environment. One of the broad transatlantic energy objectives is the realization of the Southern Corridor as the alternative fourth corridor with Caspian region resources after Russia, North Sea, and North Africa supply regions. In this context, the corridor will be connecting the Caspian Sea to Turkey and NATO allies in European continent.

More notably, in the Cold War period, experiences of NATO commanders and decision makers mostly focus on either deterring major nuclear or conventional attacks or engaging in possible military operations to guarantee oil supplies for aircraft, tanks, submarines and battle ships from the Article V. Thus, most importantly, all these reasons reflected for Allies critical alarmed mode were among the possible military threats that came from the outside of transatlantic community borders. Yet, modern

⁵¹³ NATO Alliance adopt a wider approach to energy security, that will entitle that the interests of "producer", "transit" state and "consumer" will be effectively seen in a similar light against threats that will undermine the interests of all , or should it adopt a more regional and directed one in which the interests of "producer" and "consumer" differ, which will essentially bringing the influence of a powerful Alliance to succor the "consumer" in what is considered to be a competitive dialogue between "producer" and "consumer". A. Monaghan, "Energy Security – What Role for NATO?", *NATO Defence College Research Paper*, No. 29. September 2006.

⁵¹⁴ At the Riga summit, Heads of State and Government called for a "coordinated, international effort to assess risks to energy infrastructures and promote energy infrastructure security".

societies have realized that newly emerging energy risks cannot be met by the use of traditional means of security in today's quickly globalizing world.

From one very important aspect, international security environment added a new layer of non-predictable threats. Post-modern energy security environment should have certain capabilities such as being global and unpredictable, readiness, flexibility and sustainability in order to meet the very complex challenges just behind the borders of sovereign states. Presently, NATO is faced with natural disasters, tsunamis and climate changes which have trans-boundary impacts as well as human risks and non-state actors using new tactics of cyber attacks, international terrorism, ethnic insurgent tactics, maritime piracy, and physical attacks on energy pipelines, harbor facilities and ships; reflecting the nature of transforming real challenges. Terrorist groups will always be looking for targeting the weakest points to attack and some have declared against economic aspects particularly. This is relevant to the energy security question as attacks anywhere would have destabilizing effects on NATO countries' economies and energy supplies. Generally, pipelines in NATO countries have a low probability of attack as they are the last choice of target for terrorists.

Riga Summit and Turning Point for NATO CIP Plans

When we look from the real politics perspective, the concept of critical infrastructure protection is a timely endeavor of high complexity because it rapidly increases its technological sophistication of energy infrastructure assets. Because of their developing usage in our daily lives, we think that it is difficult to manage and develop comprehensive security mechanisms for their protection and cannot guarantee the protection of all facilities against new kinds of threats. Furthermore, ongoing attacks targeted at energy infrastructure have increased over the last decade, a trend that is correlated with the growing political and economic instability in oil and gas producing regions. Data acquired from the Energy Infrastructure Attack Database (EIAD) show that in the last decade there were, on average, nearly 400 annual attacks carried out by armed non-state actors on energy infrastructure worldwide; a figure that was well under 200 prior to 1999.⁵¹⁵ From this point of view, observing from the global platforms, critical infrastructure often runs across national borders and the terrorism threat cannot be sufficiently contained by one country alone.

These fresh examples show the dimensions how concerns and threats are being discussed by NATO and where governments, political, academic and military decision makers have to cooperate in precedence route maps. In this regard, NATO allies may

⁵¹⁵ This data reveals a global picture whereby violent non-state actors target energy infrastructures to air grievances, communicate to governments, impact state economic interests, or capture revenue in the form of hijacking, kidnapping ransoms, theft. And, for politically motivated groups, such as those engaged in insurgencies, attacking industry assets garners media coverage serving as a facilitator for international attention. Jennifer Giroux, Peter Burgherr, Laura Melkunaite, "Research Note on the Energy Infrastructure Attack Database (EIAD)", *Perspectives on Terrorism*, Vol 7, No 6, 2013, <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/315/html>

confront with critical infrastructure protection mechanisms that can disconnect energy supply links or damage distribution centers while it is very difficult to identify and respond to hazardous attacks, in an unknown period of time. Accordingly, all of these vital developments under the name of security policies have led NATO allies to start planning more serious perspectives for their energy future in order to avoid crises and to make energy policy a higher priority within the Euro Atlantic region. At the Riga Summit in November 2006, NATO Heads of State and Government confirmed the Alliance's role in Critical Infrastructure Protection (CIP), reiterating their "determination to protect our populations, territories, infrastructure and forces against the consequences of terrorist attacks" and underscoring that "security interests of the Alliance can also be affected by the disruption of the flow of vital resources". Of course, Riga Summit⁵¹⁶ has reflected some new understanding of the vital interests of NATO in focusing on energy critical infrastructure protection security, rather than other dimensions of energy security.⁵¹⁷

NATO requires the development of rapidly evolving physical and technical challenges of energy infrastructure protecting a network among allied states. NATO leaders recognized energy security essentials at the Strasbourg-Kehl Summit in April 2009 and the Lisbon Summit in November 2010. Allies have identified the following five key areas where NATO can provide added value:

- Information and intelligence fusion and sharing;
- Projecting stability;
- Advancing international and regional cooperation;
- Supporting consequence management; and
- Supporting the protection of critical infrastructure.

NATO could serve as a strong democratic platform for developing such activities to defend against energy threats. NATO may be an important element for exchanging information and best practices, raising awareness and harmonizing allies' approaches to critical infrastructure protection as well as providing advice and training to improve preparedness and build resilience. Cooperation with NATO partner countries contributed to this work. Senator Richard also called for transparency and public dialogue with national democratic constituencies: "In the field of critical infrastructure

⁵¹⁶ "As underscored in NATO's Strategic Concept, Alliance security interests can also be affected by the disruption of the flow of vital resources. We support a coordinated international effort to assess risks to energy infrastructures and to promote energy infrastructure security. With this in mind, we direct the council in permanent session to consult on the most immediate risks in the field of energy security, in order to define those interests where NATO may add value to safeguard the security interests of the allies and, upon request, assist national and international efforts." NATO Riga Summit Declaration, Paragraph 45. <http://www.nato.int/docu/pr/2006/p06-150e.htm>

⁵¹⁷ Summit in Riga at the end of November, energy security will increasingly be a strategic concern for the Alliance. However, it is too early to determine which roles NATO could and should play. There will need to be further discussion among the Allies before NATO's role and contribution can properly be defined.

protection, NATO, in a way, bears a soft power to invite nations to behave in a cohesive way and show solidarity amongst Allies because of mutual interests. It is a matter of diplomacy for NATO towards its own member states as well as a wide range of partner countries which is a big asset of NATO.⁵¹⁸

We can indicate for NATO military policy makers to enlarge new communication opportunities, communicate with local civilian crisis management experts more closely and more regularly to ensure the effective incorporation of their experiences and capabilities from the new NATO planning processes. What kind of new threats and challenges could emerge for the NATO maritime energy transport lines? NATO sees possible terrorist attacks by non-state actors against Allied countries' critical ports and their oil and LNG energy facilities, and sabotage possibility against high interest energy transportation (coal, oil, LNG) vessels, the use of ships and their cargo as weapons as well as the import of weapons of mass destruction, and many others. In order to maintain sustainable industrial development in NATO countries, ensuring the security of energy maritime transportation requires hard work without any interruption such as oxygen inputs from the conducted search and disaster response operations. But we have to pay attention that most of the attacks to critical energy infrastructure could often damage pipelines that carry fossil fuels within national borders or on the high seas, affect cross-border infrastructure.

NATO policy and plan makers aim to counter these possible non-clear threats and to make the NATO Alliance maritime transportation system safe. In this context, from the understanding of NATO's Smart Defense project on harbor protection⁵¹⁹, Allied countries intended to develop new Harbor Protection Capability that can be deployed quickly and used by the Allies to allow NATO maritime forces in operations to safely operate within a port regardless of the amount and quality of support capabilities by the host nation. 70% of the surface of the Earth is covered with water, 90% of global trade and about half of the world's oil is transported by sea. Maritime areas also provide a vital dimension of European economy. It is estimated that 90% of the European Union (EU)'s external trade and 40% of internal trade is transported by sea. About 350 million passengers and 3.5 billion tons of cargo per year pass through European seaports and the European waterways including a number of chokepoints such as the English Channel, the Danish Straits and the Strait of Gibraltar.⁵²⁰ NATO could carry out

⁵¹⁸ "The World in 2020 – Can NATO Protect Us?", *The Challenges to Critical Infrastructure Conference Report*, 10 December 2012, Brussels, NATO Emerging Security Challenge Division, http://lgdata.s3-website-us-east-1.amazonaws.com/docs/1494/764045/ESC_Conference_2012_12_10_FINAL.pdf.

⁵¹⁹ Smart defence is a concept that encourages Allies to cooperate in developing, acquiring and maintaining military capabilities to meet current security problems in accordance with the new NATO strategic concept. Therefore, NATO smart defence means pooling and sharing capabilities, setting priorities and coordinating efforts better.

<http://www.nato.int/docu/review/topics/en/Smart-Defence.htm>

⁵²⁰ The development of a Maritime Security Operations (MSO) Concept and a new Alliance Maritime Strategy (AMS) was endorsed by the North Atlantic Council in the spring of 2009. <http://www.nato-pa.int/default.asp?SHORTCUT=2087>

interdiction military operations explicitly designed to secure the supply of oil and gas in an actual crisis or conflict situation. NATO interdiction operations could involve short-term maritime escort operations, protecting oil rigs and terminals, assisting national authorities to protect port loading/off-loading facilities, refineries and storage sites.⁵²¹

Emerging Cyber Threat and NATO's New Security Policies

Recently, there is a highly critical reality of cyber attacks against critical infrastructure in energy facilities. Cyber attacks⁵²² have emerged as a serious threat to the energy supply systems of all allies. In recent years, there have been an increasing professionalization of cyber crimes; there have been more state-sponsored disruptive cyber attacks, and technologically sophisticated critical infrastructure such as smart grids in electricity networks that have become more vulnerable. The threat to these infrastructures is essentially manmade, but until recently cyber terrorism and cyber warfare were considered as a relatively abstract threat.

So far, terrorist networks have used the Internet mostly as a tool for intelligence gathering, recruitment and fundraising activities. Cyber attacks, including the ones against government computer systems, have been isolated and have come essentially from unstructured hackers with no ideological motivation. There were only a few instances of politically-motivated attacks.⁵²³ This critical situation could increase the danger of cyber attacks in the future. This was a good reason for NATO to incorporate protection against cyber attacks in its strategic analysis into defense planning procedures. Regarding NATO's possible cyber security obligations: When and how can cyber attacks significantly damage critical infrastructure? Does NATO seriously concentrate and worry too much about the risks of cyber attacks? What capabilities might be provided to Allies experiencing a cyber attack?

We must keep in mind that during the Cold War, NATO was protecting its communication and information architecture against the electronic threats of the Warsaw Pact. NATO had suffered its first publicized cyber attack in 1999 to protest the air strikes against Serbia. From the political agenda for the first time; cyber defense was discussed in 2002 Prague Summit. However, it failed to prevent attackers from shutting down virtually all of Estonia's internet systems in 2007.⁵²⁴ For Alliance

⁵²¹ Jamie Shea, "Energy Security: NATO's Potential Role", <http://www.nato.int/docu/review/2006/issue3/english/special1.html>

⁵²² The term describes a particular attack that aims to steal intellectual information or to cause a specific damage to the states or organizations. After deploying into the network, these intrusions stay for a significant period of time, evade conventional firewall and antivirus capabilities, and enable adversaries to gather crucial information. Hutchins, Eric M, Clopperty, Michael J. Amin, Rohan M, "Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" pp. 2, November 21, 2010.

⁵²³ 162 CDS 07 E rev 1—"The Protection of Critical Infrastructures", <http://www.nato-pa.int/default.asp?SHORTCUT=1165>.

⁵²⁴ Estonia-type cyber attacks were impact on Estonia was limited to preventing users from remotely accessing some services such as banking.

members, cyber threat targeted at security network is one of the most serious economic and national security challenges. NATO has prepared the ‘Strategic Concept’ in 2010 and revised it in 2011. This concept was aimed to “further develop our ability to prevent, detect, defend against and recover from cyber attacks...” by expanding its capacity in cyber security. NATO Member States reinforced the importance of international cooperation in the Chicago Summit Declaration of May 2012.⁵²⁵ NATO developed the smart grid cyber security in order to protect the information systems of allies, improve their defense ability against sophisticated and agile cyber threats, and reduce possible cyber-space attack threats from legal norms where meeting cyber security needs is no easy task.

The implementation, maintenance and improvement of national cyber security comprise a range of elements. These can address strategic documents of political nature, laws, regulations, organizational and administrative measures, such as communication and crisis management procedures within a member state territory, but also purely technical protection measures. Furthermore, awareness raising, training, education, exercises and international cooperation are important features of national cyber security.⁵²⁶ Why is this important during a cyber attack against critical infrastructures? Which international law norms apply to those responses from the cyber domain?

Under this perception, in order to formulate a common understanding within the Alliance, law enforcement capabilities were planned to be strengthened against cyber crime, deterring potential adversaries from taking advantage of members with vulnerabilities. This critical framework also requires a multilateral approach and a legal mentality which includes counter cyber defenses and harmonization capability for national strategies.⁵²⁷ Secondly, NATO seek to provide assistance to member states by working together for responding to cyber attacks and emergencies using advanced security capabilities in order to recover quickly from cyber attacks against their national networks, both civilian and military infrastructures.⁵²⁸

⁵²⁵ ‘[t]o address the cyber security threats and to improve our common security, we are committed to engage with relevant partner countries on a case-by-case basis and with international organizations [...] in order to increase concrete cooperation.’ Chicago Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, at para. 49, available at http://www.nato.int/cps/en/SID-D03EFAB6-46AC90F8/natolive/official_texts_87593.htm?selectedLocale=en.

⁵²⁶ Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012.

⁵²⁷ There is a need for coordination among member states on defining use of force under Article 4 of NATO’s charter. While the UN charter does not directly apply to NATO, it does affect member states. Therefore it is important to identify when computer network attacks amount to armed attacks under Article 51 of the UN charter, and by extension Article 5 of the Washington Treaty.

⁵²⁸ In order to the protection mission of NATO’s electronic systems allies has been realize the new task force, one is the NATO ‘Cyber Defence Management Board’ (CDMB), which

From the operative perspective, NATO aims to realize some critical initiatives. First, cooperation with all member states is important for organizing, creating and enforcing a security standard about those national cyber systems, which are vital for the effective functioning of the whole alliance. NATO will also provide consolidated informative advice to allies. Secondly, NATO is planning to prepare a cyber security response plan and initiate a dialog to enhance public-private partnerships. In order to accomplish this critical purpose, all members have created a common mechanism to exchange information about incidents and newly identified threats. This includes collaboration on a number of fronts including optimized information sharing, situational awareness, and secure interoperability based on agreed sets of common standards. Thirdly, member states could establish ‘Rapid Reaction Teams’ (RRTs) to be dispatched to a member state asking for assistance in case of cyber attacks.⁵²⁹ However, despite this, some members have avoided developing cyber strategies and tools, fearing the high costs of doing so; but some of them still lack basic information on the evolving nature of cyber threats and different types of possible attacks.⁵³⁰

Conclusion

There is a new NATO policy for the development and improvement of more reliable energy-related critical infrastructure protection, also the use of particular energy resources or the development of alternative fuels and technologies in the long term. Therefore, we need to discuss about a common definition of critical infrastructure in order to identify our most valuable assets and analyze vulnerabilities. Finally, we need to assign clear responsibilities of protection to various stakeholders on the national and international level including the private business community.⁵³¹

In order to answer emerging security challenges, NATO may prefer to use its soft power besides hard power by providing a solid forum to discuss critical infrastructure protection. This option may be beneficial in cost-effective terms to create common understanding atmosphere among the member nations for raising awareness about these threats. This policy preference may be realized within the legal framework of the agreement on sharing current capabilities to meet these challenges collectively in the understanding spirit of solidarity. We think, NATO should upgrade its analytical tools to gain a better understanding of the significant correlation between physical conflicts

responsible of those representatives of different NATO structures, who are responsible for cyber security. Secondly, NATO has established a “Computer Incident Response Capability” (NCIRC) to act as an in-house emergency response team. It has been tasked with evaluating security of NATO’s networks and disseminating information on incidents and threats to individual systems’ administrators. Most importantly, it will provide expertise and technical services in case of attacks against NATO’s networks.

⁵²⁹ J. Healey, L. van Bochoven, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow”, *Atlantic Council Issue Brief*, February 27, 2012.

⁵³⁰ Julianne Smith, “NATO Must Get More Serious on Cyber Security”, *Atlantic Council*, February 6, 2014, <http://www.atlanticcouncil.org/blogs/natosource/nato-must-get-more-serious-on-cyber-security>

⁵³¹ Lieutenant General Walter E. Gaskin, Deputy Chairman of the Military Committee, NATO

and increasing cyber attack activities in order to determine the most effective points and instruments for intervention. The Alliance should generate stimulating ideas about deepening civil-military cooperation in crisis management operations. This would imply stronger operational capabilities of NATO in the field of emerging security challenges. As a result, we can say that we can only achieve reasonable security purposes in collective behavior since we are living in the modern world with a dangerous and unpredictable environment.

REFERENCES

KLIMBURG, A. (Ed.), **National Cyber Security Framework Manual**, NATO CCD COE Publication, Tallinn, 2012.

MONAGHAN, A., “Energy Security – What Role for NATO?”, *NATO Defense College Research Paper*, No.29, September 2006.

GIROUX, J., BURGHERR, P., MELKUNAITE, L., “Research Note on the Energy Infrastructure Attack Database (EIAD)”, *Perspectives on Terrorism*, Vol.7, No.6, <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/315/html>, 2013.

HEALEY, J., VAN BOCHOVEN, L., “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow”, *Atlantic Council Issue Brief*, 27 February 2012.

SHEA, J., “Energy Security: NATO's Potential Role”, 2006.

SMITH, J., “NATO Must Get More Serious on Cyber Security”, *Atlantic Council*, 6 February 2014.

NATO Riga Summit Declaration, Paragraph 45,
<http://www.nato.int/docu/pr/2006/p06-150e.htm>

NATO Emerging Security Challenge Division, “The World in 2020 – Can NATO Protect Us?”, The Challenges to Critical Infrastructure Conference Report, 10 December 2012, Brussels.

IMPLEMENTING CYBER SECURITY ACCORDING TO NATIONAL REGULATIONS AND INTERNATIONAL STANDARDS

Kristina SANDER

Guido GLUSCHKE

ABSTRACT

The threat from cyber-attacks is increasingly perceived as a problem of national and international security as cyber-attacks grow in number and sophistication and as perpetrators are no longer only private hackers or organized criminals, but also nation states. In consequence, international organizations seek to find good standards and practices for their member states in order to regulate cyber security for critical infrastructures, such as energy, in an adequate way. The European Union (EU) has published a directive on security of Network and Information Systems (NIS)⁵³² in 2016 forcing their member states to implement a cyber security regulation on all critical sectors. Germany as one of the EU member states adopted a new legislation on cyber security within national critical sectors in 2015, named IT Security Act. Energy was one of the sectors covered. The new legislation led to a couple of new regulations which now come from different authorities with overlapping responsibilities and partly existing regulations. The status of the German regulation in the energy sector will be discussed in this paper and a way for implementing the regulation on Transmission System Operator (TSO) or Distribution System Operator (DSO) side will be shown.

Key words: Cyber Security, Regulatory Framework, Security Management, Cyber Security Energy, TSO, DSO, EU NIS Directive, Information Security Management, ISO 27001

Introduction

Today, all industries are becoming more and more digitalized. The energy and the nuclear sector are no exceptions from this trend. Information and communication technology is part of most business processes and influences the energy sector in the same way as it does other industries. The relevance of digitalized technology and the consequences following this innovation process has led the nation states and international bodies to discuss new laws and regulation on cyber security.

⁵³² Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Internationally, initiatives on cyber security can be seen in different organizations, such as the International Atomic Energy Agency (IAEA) or the European Union (EU). The IAEA, focusing on nuclear energy, worked since 2003 on a document which should guide their nation states to regulate computer security at nuclear facilities and which was published in 2011 as NSS 17⁵³³. A couple of further documents regarding cyber security exist in between within the IAEA Nuclear Security Series (NSS). The approach of the EU is more comprehensive, not limited to energy, and covers critical infrastructures in a broader sense. This paper looks closer to an implementation of the EU approach in the energy sector. For the energy sector the NIS directive covers the electricity, oil and natural gas subsector. Even if many people at the European Commission think that nuclear energy is included in the NIS directive, there are other opinions on that. Also the Energy Expert Cyber Security Platform (EECSP) - Expert Group covered nuclear as a subsector in its report⁵³⁴ which came out early 2017. But being very precise, nuclear energy is not covered by the text of the NIS directive, still there is no reason for a nation state to exclude it when implementing NIS. Hereinafter is illustrated how Germany included nuclear energy as part of electricity, under their NIS directive. And there is a good reason why, which will be discussed later.

EU Regulative Framework

The EU NIS directive was the first EU-wide legally binding set of rules on cyber security. It can be seen as a regulatory framework for its member states. The objective of the NIS directive is to achieve a high common level of security of network and information systems within the EU through

- improved cyber security capabilities at national level,
- defining the strategic objectives, governance framework, appropriate policy, regulatory measures,
- introducing national competent authorities to monitor the application of the directive at national level,
- single points of contact to ensure cross-border cooperation.

To achieve these objectives distributed responsibilities are defined for different stakeholders, for example:

Member states are obliged to adopt a national strategy on security of network and information systems and to establish a related national Competent Authority (CA). Appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems have to be implemented by the member states.

⁵³³ International Atomic Energy Agency, IAEA Nuclear Security Series No. 17 – Computer Security at Nuclear Facilities, Vienna 2011.

⁵³⁴ Cyber Security in the Energy Sector - Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP-Report, European Commission, Brussels, Feb 2017

National Computer Security Incident Response Team (CSIRT) should monitor incidents on national level, provide early warnings and alerts to relevant stakeholders and respond to incidents.

Increased EU-level cooperation should exchange information among member states within a Cooperation Group on European level with national experts. In addition, CSIRT networks should be developed.

The European Union Agency of Information and Network Security (ENISA) should plan and steer work programs, assist and support member states, discuss and evaluate national strategies and should share information and best practices on threats and risks, incident handling, training, etc.

Operators of essential services which are those organizations able to generate significant disruptive effects to economy or society have to be identified by the member states. Member states have to ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems. Incident reporting obligations for operators of essential services and digital service providers exist.

The national implementation of the EU NIS directive has to be adopted by 9 May 2018.

Germany's response to the EU NIS directive

The German approach is a multi-step approach in terms of developing and implementing cyber security regulation in all critical sectors. The composition of national critical infrastructure, comprising the relevant operators of essential services, consists of eight private sectors shown below:

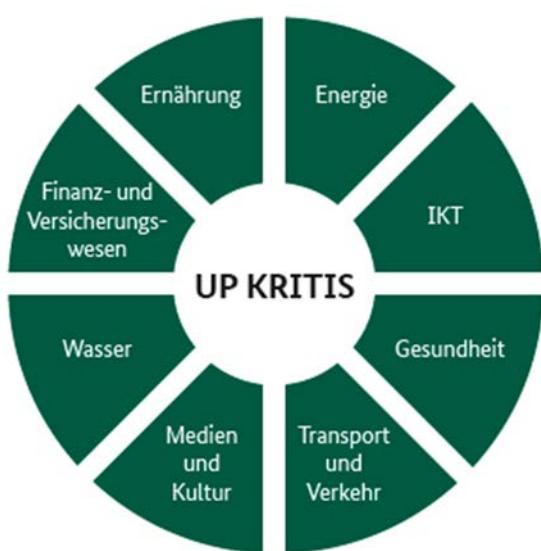


Figure 9 –Germany's sectors of critical infrastructure

The state's owned infrastructure necessary for the government is not included as there are other national programs to protect this infrastructure. Most sectors are allowed to develop their own sector-specific cyber security standards which then have to be evaluated by Germany's competent authority named Bundesamt für Sicherheit in der Informationstechnik (BSI). A few sectors are not allowed to develop their own cyber security standard, such as the energy sector. Their regulation comes from ministries or governmental agencies.

For the energy sector two regulators exist. On the one hand, nuclear energy is regulated by the Ministry of Environment, the Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB). The BMUB issued its first cyber security regulation for nuclear power plants in August 2013. This regulation called SEWD-IT required adequate protection against interference or other effects of third parties on IT component but did not consider the upcoming EU NIS directive. It describes how cyber security has to be organized by particular nuclear facilities in regards to the nuclear security goals which are protection against theft and release of nuclear material by using results of the Design Basis Threat methodology⁵³⁵. Nuclear storing facilities, facilities in construction, in operating or in a decommissioning phase as well as reprocessing facilities and facilities with other use of nuclear material, such as research facilities, were affected by the regulation. The implementation of the SEWD-IT has to be enforced by the Federal States in Germany.

On the other hand, cyber security for energy production and transport is regulated by the Bundesnetzagentur (BNetzA). The BNetzA is a specialized agency of the Ministry of Economy, the Bundesministerium für Wirtschaft (BMWI). The BMWI issued the Energy Industry Act (EnWG) which requests a reliable offer of energy by the energy operators. The goal, defined in EnWG §11, is translated by the BNetzA into a new regulation called IT Security Catalog, published in August 2015. This regulation is a sector specific response to the requirements given in the German IT Security Act which was issued by the Ministry of Interior (BMI) some months before. The first version of the IT Security Catalog that time was issued only for energy grid operators, so called Transmission Service Operator (TSO) or Distribution Service Operator (DSO). For nuclear and non-nuclear energy generation facilities a similar regulation of the BNetzA is expected in 2018. In opposite to the BMUB regulation for the nuclear sector the BNetzA regulation focuses on reliability of energy and with that extends the scope of the existing regulation on cyber security for the nuclear sector as reliability of energy is not a goal within the SEWD-IT regulation. By today, the SEWD-IT can be seen as part of German's cyber security framework under the IT Security Act which, to be precise, was a collection of changes to existing laws, such as Energy Industry Act or Nuclear Act, and is not an own-standing German law. In addition, an operator is categorized as critical infrastructure if it exceeds particular threshold values given by the BSI⁵³⁶.

⁵³⁵ International Atomic Energy Agency, IAEA Nuclear Security Series No. 10 – Development, Use and Maintenance of the Design Basis Threat, Vienna 2009.

⁵³⁶ German Regulation on Cyber in Critical Infrastructure: BSI-Kritisverordnung 1. Teil, BSI, March 2016

An overview of the German regulation for the energy sector can be seen in the following figure.

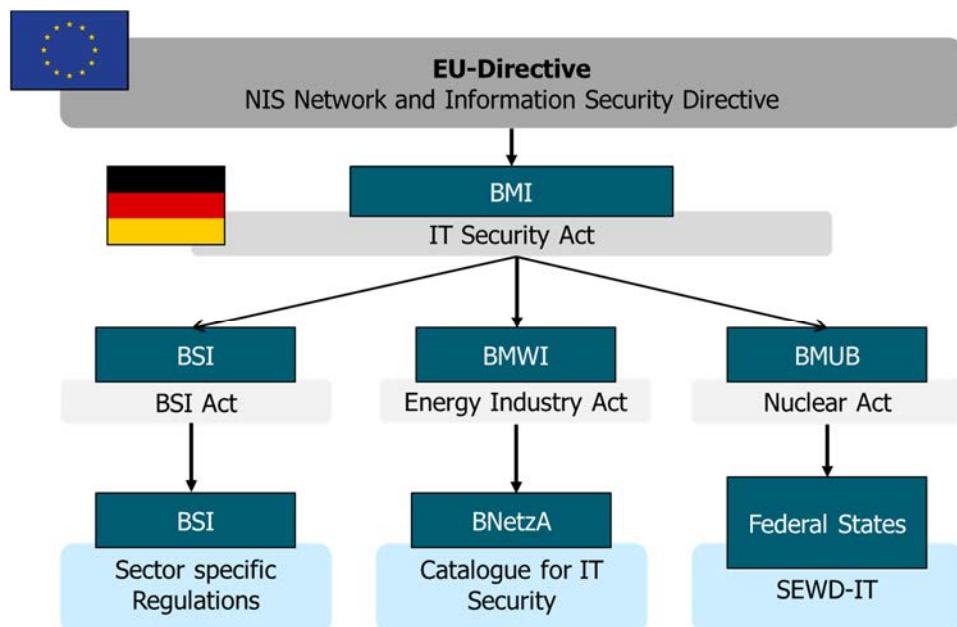


Figure 10 – German implementation of EU NIS directive for the energy sector

With the IT Security Act German's competent authority for IT security (BSI) became the single point of contact in Germany for any kinds of cyber-related incidents from the critical infrastructure community. A duty of notification for operators of critical infrastructure was introduced in case a cyber incident was considered to disrupt essential services or even did it. Also the operators had to appoint single points of contact in order to establish a bidirectional way for communication from and to the BSI. The protocol for communication regarding a cyber incident was defined by the BSI and is quite comprehensive.

Germany's cyber security regulation for energy grids

As mentioned above the IT Security Catalogue is German's regulation for energy production using gas and power and regulates within EnWG §11 part 1a cyber security for energy grids and in part 1b cyber security for energy generation, nuclear and non-nuclear, fossil and renewable. These are two different documents, both called IT Security Catalogue.

This paper focuses on the IT Security Catalogue for energy grids as the other one for energy generation is not published yet. The scope of the existing IT Security Catalogue for energy grids applies on all central and decentralized components, applications and systems relevant for a secure network operation in order to ensure reliable energy transmission and distribution. It asks operators for a secure energy network operation including appropriate protection against threats coming from telecommunication and

electronic data processing systems, which are necessary for a secure network operation.

The way which was chosen by the German regulator (BNetzA) to ensure cyber security in the energy sector was based on the idea of using an ISO/IEC 27001 Information Security Management System (ISMS). Such a management system can be seen as an instrument to ensure a constant level of quality and effectiveness of security which then has to be satisfactorily shown in an audit resulting in a certification of the implemented ISMS.

To reach a certification a couple of supporting standards, such as ISO/IEC 27011, the BDEW Whitepaper or the BSI ICS Compendium can be used to implement a robust cyber security regime on operator's side.

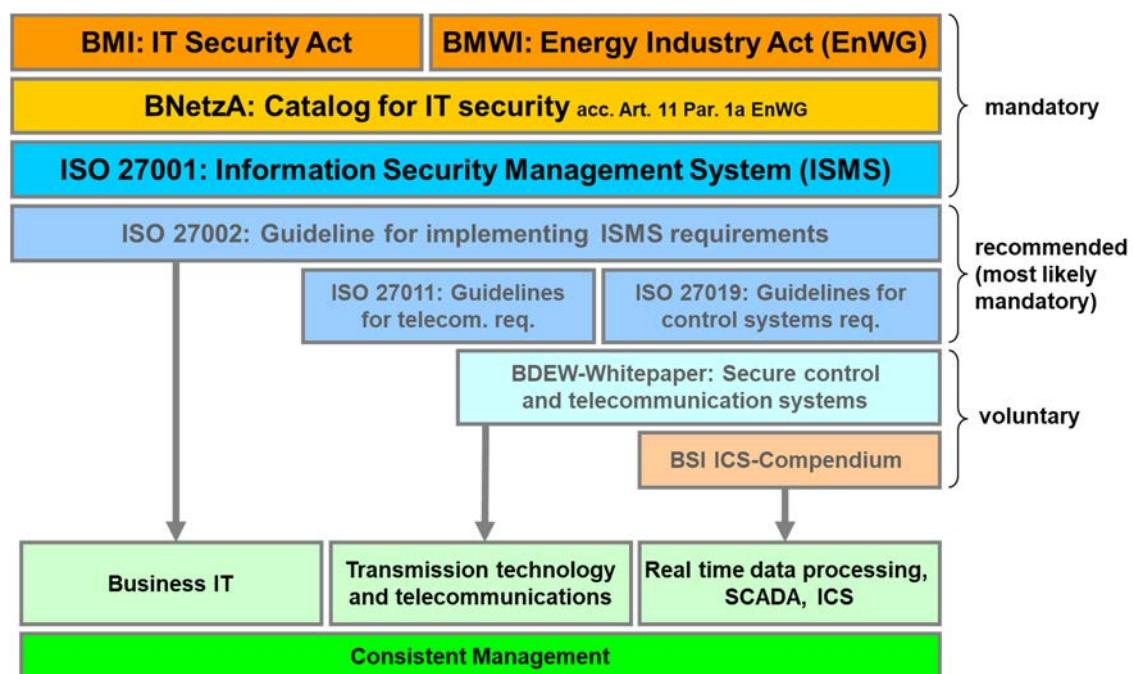


Figure 11 – German cyber security regulation framework for the energy sector

Beside the legal basis the IT Security Catalog describes the cyber protection goals, the scope, security requirements, the information security management system, security categories and controls, the requirements for the map of the network structure, the risk analysis and treatment process and the point of contact for IT security as well as the certification process and the timeframe for implementing the regulation.

As mentioned, the IT Security Catalog request the operator to establish a holistic information security management system (ISMS) according to ISO/IEC 27001 together with ISO/IEC 27002, extended by specific requirements of ISO/IEC TR 27019, information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. The extensions specific to the IT

Security Catalog focus on the structure of the IT used in grids, considers specific threats and require the implementation of state-of-the-art measures.

For all IT systems which are in the scope described by the IT Security Catalogue a map of the network structure has to be presented which shows an overview of components, applications, systems affected by the scope of the IT Security Catalogue. All IT components in scope have to be documented and categorized in one of the following three categories:

- Main Control systems: Every centralized system which serves for control or monitoring of the energy network as well as supporting IT systems, applications and, central infrastructure, such as central systems for control and monitoring of operations, central systems for measurement, systems for supervision and control of energy network storage, systems for data archiving, central systems for parameterization, configuration and programming and every system which is necessary for aforementioned operations.
- Systems for transmission or communication: Technology which is used for communication or transmission, telecommunication and networking, such as router, switches and firewalls, network elements of transmission technology, centralized management systems and supervision systems for transmission, telecommunication and network technology, communication terminals, mobile, cell and wireless systems.
- Safety systems, automation and remote control systems: Technologies which are close to the processes of control and automation, protection and safety systems, including components of remote control; especially the technology in decentralized stations and the automation technology for energy network storage systems, such as control and automation components, field devices, controller, PLCs, digital sensors and actuators, devices of protection and security components, remote control and remote operating devices, systems for measurement.

IT components, applications and systems which are in the scope has to be analyzed regarding particular threats and risks. The IT Security Catalog defines specific requirements for the risk management process. Risk management is governed by specifications on classification criteria for impact, such as:

- impairment of supply security,
- restriction of energy flow,
- share of population affected,
- threat to life and limb,
- impact on other infrastructures (e. g. up- or downstream grid operators)
- impact on data security and data protection arising from disclosure or manipulation,

- financial impact.

After the risks are analyzed the risk treatment process allows the operator to consider economic aspects when making decisions on the effectiveness and implementation of cyber security measures.

Finally, a certification has to be presented by the operator to the BNetzA by end of January 2018 which is in line with the requirements of the ISO/IEC 27001 standard and the extensions coming from the IT Security Catalog. A certification according to raw ISO 27001 would not work. A separate certification process with auditors accredited by the German Accreditation Agency has to be passed by the energy grid operators.

Generic approach for implementing a cyber security program

A generic approach for implementing a cyber security program for TSOs and DSOs according to the German regulation can be achieved through the following steps:

Firstly, a management commitment is needed. The management has to express its will to build up an Information Security Management System (ISMS). The management commitment should be expressed in an Information Security Policy, signed by the management. Roles and responsibilities for information security are determined in this document.

A definition of the scope is needed which describes which people, locations and IT systems are in the scope. One outcome is a Scope Description document. Another outcome is a structured map of the network in scope.

Then, management support is needed, financial and non-financial resources have to be offered by the management to set-up an appropriate program and to implement necessary protection measures.

A document structure has to be developed comprising all documents needed for setting up and running an ISMS. The outcome of this step is a description of the ISMS.

An inventory of assets within the scope is needed. This inventory should list all relevant assets necessary for a secure operation of the energy grid. In addition, asset owners have to be determined by the organization.

To assess the risks, a Gap Analysis is done. This structured approach assesses all non-compliant situations in the organization. The Gap Analysis is done against the ISO 27001 and ISO 27019 controls.

As part of the risk assessment a business impact analysis and a threat and vulnerability analysis has to be done. The combination of both is the risk which should be reported in a risk analysis report.

Further, a risk treatment has to be done. Decisions have to be made by the organization in order to mitigate risks in a proper way and to know which risks remain. The remaining risks have to be transparent for the organization and have to be taken by the top level of the organization.

The mitigating measures have to planned and implemented.

For improvement a performance evaluation and an audit program should be done. Audit reports and measurements of key performance indicators (KPIs) are proven instruments to get the organization more secure and more mature.

Finally, an ISO 27001 certification can be done.

REFERENCES

BUNDESVERBAND DER ENERGIE- UND WASSERWIRTSCHAFT E.V. (BDEV), White Paper Requirements for Secure Control and Telecommunication Systems, Berlin, 2008

BUNDESMINISTERIUM DES INNERN (BMI), German IT Security Act: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Berlin 2015

BUNDESNETZAGENTUR (BNetzA), German IT Security Catalog: IT-Sicherheitskatalog, Bonn 2015

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), ICS Security Compendium: ICS Security Kompendium, Bonn 2013

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), German Regulation on Cyber in Critical Infrastructure: BSI-Kritisverordnung 1. Teil, Bonn 2016

EUROPEAN COMMISSION, Cyber Security in the Energy Sector - Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, EECSP-Report, Brussels 2017

EUROPEAN COMMISSION, Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, Brussels 2016

INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Security Series No. 10 – Development, Use and Maintenance of the Design Basis Threat, Vienna 2009.

INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Security Series No. 17 – Computer Security at Nuclear Facilities, Vienna 2011.

INTERNATIONAL STANDARDIZATION ORGANIZATION (ISO/IEC), 27001, Information technology — Security techniques — Information security, management systems — Requirements, Geneva, 2013

INTERNATIONAL STANDARDIZATION ORGANIZATION (ISO/IEC), 27002,
Information technology — Security techniques — Code of practice for information
security controls, Geneva, 2013

INTERNATIONAL STANDARDIZATION ORGANIZATION (ISO/IEC), 27011,
Information technology — Security techniques — Information security management
guidelines for telecommunications organizations based on ISO/IEC 27002, Geneva,
2008

INTERNATIONAL STANDARDIZATION ORGANIZATION (ISO/IEC), TR 27019,
Guidance for information security management of power supply control systems
based on ISO/IEC 27002, Geneva, 2014

BALANCING CYBER AND PHYSICAL DEFENSE IN THE ENERGY SECTOR: NUCLEAR ENERGY LESSONS LEARNED

Dmytro CHERKASHYN

ABSTRACT

Even in matured utilities of energy sector protection costs could be underestimated. This problem is getting worse, when the new threats appear such as IT/Cyber threats and become credible. In such conditions companies are starting to spend huge budgets on the IT infrastructure and specialist, while leaving more space for criminals and terrorist on well-known physical polygon. To effectively balance between these two major defense fields, it is necessary to create well communicating structures, which are capable to build and sustain the unapproachable perimeter for both cyber and physical threats.

Key words: Energy, nuclear, physical, cyber, defense

Introduction

When talking about cyber defense, usually we will not find too much information about specialists for one or another sector such as water, electricity or other utilities supplier. IT/Cyber security expert are usually dealing with digital assets such as data threads, servers and clients, industrial control systems with specific types of data and commands circulating inside, rather than with the physical assets of protected domain itself as pumps, transformers or other industrial equipment. It means that they will use more or less generic approaches to organize protection of such cyber systems. For such purposes they can use variety of well-documented standards, which could be not obligatory to use at all, depending on the state of legislation development in particular country. To enhance cyber defense on critical infrastructure domains and especially Energy Sector, it is crucial to communicate with representatives of authorities and licensing authorities. Furthermore, Energy sector is going to be more and more transborder, where powerlines transmitting electricity to other countries and using shared communication channels to operate with system, considering same level of cyber security as country of origin. This requires clear understanding and use of non-ambiguous definitions.

Definitions of Energy Security itself could be very different in many contexts. Starting with Wikipedia's one, which says:

*"Energy security is the association between national security and the availability of natural resources for energy consumption."*⁵³⁷

Access to energy sources is crucial for development of economy and society in the country, but another view on Energy security problem is Energy diversification⁵³⁸ that means "*using different energy sources, suppliers and transportation routes to reduce dependence on a single resource or provider. A country that diversifies its energy mix insulates itself from energy disruptions and strengthens its energy security.*"⁵³⁹

The International Energy Agency defines energy security as "*the uninterrupted availability of energy sources at an affordable price*"⁵⁴⁰, making emphasis on affordability of the prices.

Abdelrahman Azzuni and Christian Breyer [see references] talk about up to 15 dimensions of Energy Security, which shows fundamentality of this topic. Long-term energy security term usually deals with healthy economic development in the frame of increasing energy needs. Short-term energy security more focuses on the ability of the energy system to react promptly to sudden changes within the supply-demand balance. Lack of energy security is thus linked in long-term to the not competitive or overly volatile prices and negative economic impacts or in short-term to social impacts of physical unavailability of energy. Thus, last one is most appropriate to cyber defense topic, while usually is main intention of hackers.

Nuclear Energy is a part of critical infrastructure and bears many risk associated with relying on it starting with nuclear terrorism risks, international proliferation risks and energy security risks for some countries and regions. As not typical sophisticated production domain, Nuclear Energy has its own safety and security issues. To understand what kind of threats Nuclear Security handle, we should again return to definitions.

Considering that original idea of nuclear use was for strictly military purposes, it had transferred into civilian application many risks, thus, creating different flows of Nuclear Security discussions.

As expected, one of definitions, given to Nuclear Security, is related to the state national security and maintenance of nuclear weapons as its important part. Of course, there is reverse definitions exist, saying the Nuclear Security "*is global actions to reduce urgent nuclear dangers and build support for reducing reliance on nuclear weapons, ultimately ending them as a threat to the world*"⁵⁴¹.

⁵³⁷ https://en.wikipedia.org/wiki/Energy_security

⁵³⁸ http://energyeducation.ca/encyclopedia/Energy_diversification

⁵³⁹ <https://share.america.gov/diversifying-energy-sources-boosts-security/>

⁵⁴⁰ <https://www.iea.org/topics/energysecurity/>

⁵⁴¹ <http://www.nti.org/about/projects/nuclear-security-project/>

One more, neutral to others, it is benefits derived from nuclear power: the energy security and the environmental security which our world will so urgently need in the 21st century and which nuclear power is uniquely able to deliver on a global scale.

There are few others, which are basically right, but we will use internationally approved definition of Nuclear Security from IAEA, which is *the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities*.⁵⁴²

Nuclear Security has more than three decades history, where most time specialists operated with Physical Protection term as main one and considered physical assault on Nuclear Facility as one of the most credible scenario. Under pressure of international community and regulators, operators have no other way than develop heavy physical protection systems, which development experience can give us examples of good practice.

Unfortunately, about decade ago the world had met another huge threat with faces of industrial digital components and hackers, who know how they are working and weak points of system. If earlier main consideration was about business units with financial data, now it also touches SCADA servers and other devices, access to which gives opportunities to change process parameters and potentially cause sabotage.

What causes more financial lose: physical or cyber?

The worry that terrorists, criminals or state actors may penetrate into control systems and use them to cause power outages, severe damages of oil pipelines, or harm medical facilities exists since 9/11 happened. Of course, in real life it is much harder to do than it sounds, which basically explains why so far we have seen only few power outages triggered by a cyber-attack in the world.

While many thousands of small non-sophisticated attacks are firing control systems in the world every day, wild animals and fallen trees branches have done much more damage and money loss. Many of equipment are located in distance from any control centers and very often have a weak surveillance and physical protection. These factors make it attractive for criminals and terrorists, while they don't need to possess of any sophisticated skills and knowledge to steal valuable metals from such places or disrupt its normal operation.

*"In Iraq, terrorist groups have skillfully used their resources and insider contacts to repeatedly attack national power transmission, to cause both disruption and social unrest and also to steal valuable materials such as copper conductors."*⁵⁴³

⁵⁴² <http://www-ns.iaea.org/standards/concepts-terms.asp>

⁵⁴³ <https://www.nap.edu/read/12050/chapter/5>

“Similarly, terrorists have been physically attacking Colombia’s electrical grid at a rate of over 100 times a year with different level of success.”⁵⁴⁴

From US Energy Incident Data Base it’s known “*that from November 1, 1996, to November 1, 2006, 528 substations were attacked worldwide. This number includes substations and switchyards collocated with substations that were attacked with rocket propelled grenades (RPGs), mortars, small arms, etc. For the same 10-year period, 2,539 transmission towers were attacked worldwide (attempted attacks)*”.⁵⁴⁵

Another problem, which appears suddenly, it is domestic terrorism. One of the very indicative cases had happened on April 16, 2013 in US; when some people snuck up on local substation in Metcalf, California.⁵⁴⁶ As said, they cut fiber-optic AT&T phone lines and fired more than 100 rounds of rifle ammunition into the radiators of 17 electricity transformers. Thousands of gallons of oil leaked, causing electronics to overheat and finally shut down.

As result, this short 19 minutes assault caused \$15 million in damage and revealed serious physical security issues. Transformers are very often custom designed, sometimes costing \$3 million each -- and replacements are slow. Plus, physical attacks on energy distribution machines are much more effective at taking out the power grid than a computer hack. It is still one of the most worried issues for energy utility firms.

Another case happened in Ukraine, when only two explosions of power towers close to Crimea border have caused disruption of energy supply for almost 2 million people for many weeks. Regardless of the political situation, it should be not allowed to act in such way, while it is violation of National Law. In the same time, last successful cyber-attack happened in Ukraine resulted in affecting 70 to 200 thousand of consumers for one to six hours mainly in the nighttime.

Tampering and thefts from substations are daily burden for many years for whole world even for most developed countries; it is still there, there is almost zero results were achieved to prevent this. Cyber-attacks become also more complex and well planned, but still happened mainly because of weak security culture and lack of awareness training for staff.

Development of unmanned aerial vehicles as hobby for many people and relatively weak control for technologies makes it another potential way to deliver disruption of remote substations. Some non-severe accidents happen time to time, but intentional sabotage using such UAV could cause dramatic harm for companies.

Another way to develop an attack is use physical equipment to upload virus or any other malicious application into the target system. This vector of attack could be also extended with replacement of original equipment on infected one or another option, but it is clear, that such successful attack will cause huge money loss and disruption.

⁵⁴⁴ <https://www.nap.edu/read/12050/chapter/5>

⁵⁴⁵ <https://www.nap.edu/read/12050/chapter/5>

⁵⁴⁶ <http://money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html>

One of most demonstrative attack called “Stuxnet” and caused disruption of long-term processes and destruction of expensive equipment for Iran’s nuclear program.

Causing disruption on Energy sector could hardly be profitable, that is why most number of such attacks is likely act of intelligence from state actors, terrorist groups or hacktivists. Fortunately, in most cases administrative networks are disconnected from operational networks, so successful ransomware attacks should not be a threat for grids. But since more control systems are connected to the web, more consumer devices could be hacked to be a part of Botnet and more unified protocols are used for industrial application, number of vectors for potential attack is increasing. As more control systems are connected to the web, more new vulnerabilities will inevitably appear in the future.

Nuclear Security Lessons Learned

Nuclear Energy is very demonstrative in the sense that mankind have been not waiting until something happened before start investing money in security. Today, nobody can say “What if we spent less money on security”, because there is no evidence of severe terrorist attacks on nuclear facilities, but on the other hand it means that level of security measures is at least appropriate.

But what is appropriate level means? Usually, it is referring to the Design Basis Threat, which is description of all potential threats that facility’s physical protection system should withstand for a given amount of time, before response forces start their activity on neutralisation of adversaries. This approach gives good result from several perspectives:

- Gives relatively defined adversary model
- Gives freedom to organize security measures according to a proposed DBT
- Gives opportunity to operator and regulator to assess effectiveness of developed security system against DBT based on system performance
- Makes possible to review and correct existing system according to changes in DBT, while they are changed once per 3-5 years.

Before 2005 Physical Protection was almost self-sufficient in term of security issues for Nuclear Facilities. IT security was mainly presented by internal security service, which deals with administrative networks and probably participated in development of operation network on the facility site, but the issue of hackers seeking control over operational networks was not so serious.

Today, international community looking for solution of arising cyber threat trying to adapt existing methodologies for Physical Protection on IT Security domain, where it is possible to achieve. It is known, that recommendations and solutions for nuclear security are almost gold standard for others domains, but considering strong Physical Protection and deep vetting for staff, it gives for Nuclear Energy advantage when talking about overall security level, comparably with other industries.

Facility Characterization and Target Identification

From the point of Physical Protection view, main target on nuclear facility was always nuclear material, but of course, we should also count vital systems for safety and still, it is only dozens of items and locations, while cyber domain will count up to thousands of digital assets around facility, which should be counted and controlled.

Another system, which dependent on digital and network components, is security system itself. Physical protection reached the state, when best balance between costs and effectiveness was found using networked systems, which makes it target for hackers as well as any other digital system. In the same time, Physical Protection is likely designed without consideration of multiple followed-up attacks, which could be performed targeting digital assets. It means that without timely response on national and international level such set of attacks could reach the target.

Despite of recommendations for structure of security zones inside nuclear facility, many zones, which should be isolated, would have potential bridges between each other, what could create vulnerabilities for vital systems. Since almost all existing nuclear facilities were commissioned more than 20 years ago, no security-by-design concepts were implemented. This mean that IT systems implemented in all management, operational and supportive processes were adapted to security recommendations, what is not always cover all critical points. On the other hand, nuclear facility extensively using HMI and many manual controls over systems, so digital controllers could be potentially compromised to change behavior of actuators when operators use them.

Threat analysis and DBT

This part will be in details covered in another article, but it is worth to emphasize most important points.

In terms of security measures, it is very important to identify all credible threats for the state, including terrorist's threat or state actors threat. Based on existing capabilities of operators in consultancy with industry experts, regulator, intelligence representatives and local police extract all threats, which operators could deal with. Usually, to define list of weapons and special tools potentially available for criminals or terrorist groups, lists of existing instrumentations are used. Based on this, DBT could be limited to a small group of people with industrial explosives and automatic rifles, or to single person with knife. Using introduced DBT and results of physical protection equipment testing again different types of weapon and tools, it is possible to match appropriate protection set with satisfactory effectiveness level.

Cyber threats are more complex issue. Since successful cyber-attack is result of target study and intelligence plus malicious code developer contribution, it is hard to define criteria for operator's cyber protection. It is worth to mention that many countries with nuclear energy still don't have any legislation and regulations for operators in term of cyber security on nuclear facilities. Any steps taken in this direction will enhance cyber defense posture for nuclear or other critical infrastructure. Discussions about

prescriptive and performance based security measures for physical protection is still appeared. Using existing IT security standards it is possible to set minimum level requirement to protect nuclear facility's IT system against basic attacks and infection methods.

Definition of Design Objectives

Digital era brings many advantages to industrial processes control and supervision, as well as integrated security systems. But in front of cyber threats operators must think again about decisions made in design of facilities and equipment.

Physical protection systems were completely independent from any administrative systems on facilities just before access control part had given chance to control personnel attendance and optimize working hours. Which itself is not bad, until part of access control server, which contains all data about access credentials connected to administrative procurement part of facilities computer network.

To identify such vulnerability bridges teams of IT and physical protection staff should cooperate and analyze adjacent subsystems together avoiding weaknesses.

Physical protection systems itself become networked digital systems, where information from access control subsystem, CCTV, intrusion detection subsystem, energy backup systems etc. circulating through central server and duplicates on local emergency alarm station. In such conditions physical protection designers should consult or include in their teams experienced IT security specialists.

Security and contingency plans

It is impossible to ensure 100% of effectiveness against potential adversaries, so security plans should be developed for both normal and emergency operation regimes. The role of the state in such plans is critical. No one protection system could withstand limitless attacks, so its sole purpose is to give response forces needed time to begin interception and neutralization. Successful cyber-attack on physical protection system could potentially give an adversary advantage, so cyber and physical protection should count with potential hybrid attack using cyber and physical weapon.

Cyber security, as a necessary part of the organization security plan, should be periodically reviewed and updated to comply with present regulations and provide appropriate level of protection.

Education and training

Initial training of personnel is essential recruitment process for any area of nuclear facility operation. It pays back every time emergency situation is happened. Structured and unbiased personnel actions reduce risks of accident development and mitigate consequences. Human factor is still very valuable even in highly precise computer control systems.

Since technologies steps further and threat landscape changes, continuous retraining and development program is necessary to support of safety and security level. Awareness raising and trainings could give fruitful results against some brutal cyber-attacks, where human factor and nescience are used by hackers to infect computer systems without hard resistance and detection.

Security “silos” issue

It seems that Cyber Threats and Cyber Protection issues moved to the first places, comparably with other issues that can affect organizational integrity and disrupt the normal operations. Companies invest tons of money in new Cyber protection hardware, sometimes even without proper analysis of their most credible threats. Physical Protection Systems could be also extremely expensive and useless, especially if they are created without consideration of all security factors in company.

Classical approach of physical perpetration to steal a physical asset or cyber-attack to perform informational sabotage is still alive, but there are much more potential scenarios exist today, including cyber-attack with physical equipment sabotage intention or unauthorised physical access to IT equipment with sabotage or intelligence intentions.

Fortunately, most numbers of Cyber-attacks are not sophisticated and long-planned operations with participation of nation states sources. Usually, you will find alone or a group of so called “Script kiddies” who were enough luck to find unprotected system and, hopefully, not the same luck to finish an attempted attack.

Usually, their attack could be stopped by just updated operation system, changed default password on the router or very basic firewall concept, so without deep understanding of scripting and prior intelligence of attacked system such “adversary” can’t really affect the organization. Despite the fact that such unsophisticated attacks could be totally eliminated, there are still tens of thousands of such successful attacks around the world. It is worth to mention that even sophisticated attacks as the BlackEnergy and WannaCry Ransomware usually start with “blunt” mail-phishing.

While private companies, governmental organizations, critical infrastructure facilities suffer from data breaches through virtual channels, physical access may pose additional risk, because it opens more channels of attack for adversaries. Cyber security become a trend and investment made by companies to close the gaps in systems not always payoffs, potential adversaries will use all possible channels for attack, including of course physical access to a system with data, if it will easier to reach.

Scenarios where adversaries use physical access to server through insider to infect the system and using cyber vulnerabilities cause physical damage to organization, or use unpatched hole in the system get the physical access to remote equipment and infect it to spread malware around connected systems, today are more likely as never before. That is why close cooperation of physical protection and cyber protection specialist is critical to withstand future attacks.

Big companies can be more vulnerable to be affected with unauthorized person inside the company with thumb drives than just a next worm attack. Additionally, there variety of spy physical devices that could be used to get access details, such as bugs, hidden video cameras, wireless keyboard sniffers or proximity card readers increasing almost without control. Also, usually security departments responsible for computer and physical protection has their own budgets and chief security officers, so nobody want to be demoted and it could be a reason of non-effective or redundant security measures. Competition reasons, lack of communication between security officers or high management faults could lead to gaps in security.

Merged security programs including cyber and physical security professionals could be more effective in the way to better analyze employee behavior, better control vendors on-site and faster react on anomalies within the system.

It could sounds strange, but contractors hired to maintain cyber systems often have almost unlimited access to building and permissions with server equipment. They can walk around and usually their identification token will have low tracking capabilities or even any, so security personnel have no idea where they are and what they are doing on the network and equipment. More than, to avoid continuous convoy with purposes to open and close cabinets with equipment and have a more faster and convenient access, room with several servers which are responsible for different subsystems could be available at any time without tracking of physical access to them. That's a huge vulnerability and it exists.

Last years was very popular to provide students competitions in cybersecurity, where students focused on protection of websites, different servers, passwords and other cyber attributes. One of such competitions was supplemented with physical access element. During the attack of hacker's team on electrical power substation, defender's team should block an attack. While most defenders were trying to discover digital vulnerabilities had used by hackers, another defender team has sent someone to check the substation, where they discovered physical access to computer system.

In some cases to get remote access from outside of facilities can demand much more efforts than just get actual physical access to the targeted system. In case of merged security team, it will show physical penetration earlier then adversary will try to get access to computer system.

For any new planning facilities, the interconnectedness of physical and digital protection should even more obvious. During design and construction, both parties of security process (physical and cyber) should be involved then they will be able to detect any potential vulnerability before system been built up. While it is not easy just join these two departments of security in one, it is not so much technical issue than just organizational problems. Top management could be now aware of interconnected risks or has a lack of believe in physical threat than in cyber. Or line management can resist to such changes, because it requires deep insight into the both field to look at the security holistically. Also, in many organizations, cybersecurity has a larger budget than physical security – and they want to keep it that way, but stimulating

communication between two types of security, companies are able to drastically enhance their protection.

Conclusion

It is impossible to be protected from all threats on 100%, otherwise it will cost much more than organization earns, but security budget is also bad indicator for security measures effectiveness assessment. Number and price of equipment and software are used as security controls can't reflect its real contribution in security level, because organizational measures could give much more effect.

To identify vulnerabilities, which could be "in between cyber and physical" it is useful to organize brainstorm for both physical and cyber security people in the same room.

Deterrence in Cyber protection world is even worse than in Physical. If your server has sticker "Protected", be sure it will be checked meanwhile, and if not – your company will pay.

Thinking about robust protection it is balancing between physical and cyber defense all the time. Overconfidence in taken security measures could cost company a data breach or physical theft.

Encryption during data transmitting only works with well-organized physical protection of recipient or sender equipment. Otherwise, it doesn't give any effect. The same issue with logical authorization for network clients, if physical access available for I/O ports, especially USB without intrusion detection, user will reveal access credentials just during authorization.

Cybersecurity is a complex fundamental problem, but ignoring it or leaving it in its IT-bound silo is wrong strategy. In fact, IT security silo concept could ignore benefits as well as risks. According to Fairchild, "Industry professionals consider the lack of convergence to be the greatest barrier in evaluating and mitigating cybersecurity risks. An organization's existing cybersecurity tools can be leveraged to secure physical security assets. Physical security can protect IT logical infrastructure. Synergy could be realized when both cyber and physical security are converged systematically, leveraging unified policies and procedures."

Raising security culture and awareness is key concept. While people, who want use Internet on their clients and don't believe in threat or believe in their awareness, will do this with or without approval, well aware personnel will not give a chance to E-Mail and Web phishers.

REFERENCES

Azzuni, Abdelrahman & Breyer, Christian. (2017). Definitions and dimensions of energy security: a literature review. Wiley Interdisciplinary Reviews: Energy and Environment. 7. . 10.1002/wene.268.

A PRAGMATIC AND STRUCTURED METHOD TO SECURE THE SYSTEMS THAT CONTROL THE NUCLEAR ENVIRONMENT

Özkan DEMIRÖZ

ABSTRACT

Malicious persons and security researchers show interest in the (lack of) security of Industrial information and control systems (ICS). Systems which are directly accessible from the internet are criticized in particular. However, ICS systems have more aspects that require specific attention. This section gives you in a pragmatic way an overview of common weaknesses and complexity of ICS environment in the nuclear industry, vulnerabilities and potential threat actors and a list of fundamental “good practice” controls to protect ICS environments in the nuclear environments.

Key Words: Cyber Security, Critical Infrastructure, complexity, weaknesses, Threat actors, Vulnerabilities, ICS Risks, Common ICS Threats, ICS vulnerability challenges, SCADA, Pragmatic, Fundamental controls

Introduction

There are different types of industrial information and control systems (ICS) (e.g. PLC, DCS and SCADA) that control and monitor industrial machinery in nuclear environments. Furthermore, an ICS may be embedded in industrial machinery, located in a remote device (be it a hand-held device, a local controller or part of an integrated system in a control room) or both. ICS are used also in industry sectors that focus on large-scale physical activities, such as manufacturing, mining, utilities and transportation. ICS can also be located in an organization’s supply chain, which can influence supply chain risks with suppliers of goods and services. ICS are often ‘mission critical’, ‘safety critical’ or support critical national infrastructure’. The control of industrial machinery has evolved from manual operation, through mechanization, to computerized ICS. In today’s modern world, ICS – sometimes referred to as operational technology (OT) – are increasingly connected to IT systems used in more traditional corporate environments. However, the technology used in these environments can be extremely different.

ICS need protection from unauthorized access, interference and damage. ICS-related information (e.g. commands to control machinery, critical monitoring data, sensitive

architectural designs and user authentication credentials) also requires protection as this information is key to operation.

The impact of a compromise of confidentiality, availability or integrity of ICS-related information (e.g. caused by a serious cyber-attack) can include severe injuries or fatalities, major disruptions to business operations, substantial financial or operational penalties and significant reputational damage. However, protection of information is often given lower priority by ICS operators, architects and engineers, whose focus is on the safety, reliability and availability of ICS and the machinery they control.

Understanding the ICS components

ICS vary in design, operation, scale of deployment and level of technical complexity, which has implications for the way in which ICS environments are protected. Understanding what ICS are, their main characteristics, how they differ and the relationship between them is essential to maintaining and improving security.

Programmable Logic Controller (PLC)

A small, single-purpose, computer-based controller that continuously monitors the state of a physical device (e.g. a water pump, receiving data from a water tank sensor and sending commands to the pump motor to perform real-time control of the water level). Other ICS-specific devices that are less sophisticated than a PLC, such as a remote terminal unit (RTU) or an intelligent electronic device (IED) are treated in a similar manner to a PLC.

Distributed Control System (DCS)

A computer-based control system that monitors and performs real-time control of multiple physical devices (e.g. sensors and actuators). A DCS (e.g. a manufacturing production line) may incorporate multiple PLCs connected on a local area network (LAN).

Supervisory Control and Data Acquisition (SCADA) system

An integrated system that monitors and controls machinery located on multiple sites, often spread out over wide areas (e.g. a national power grid or railway system). SCADA are large and sophisticated, include multiple DCSs and PLCs, with ICS components in a SCADA system often connected via a wide area network (WAN).

ICS will typically run specialized applications and use dedicated real-time operating systems (RTOS). Larger ICS (e.g. SCADA) can incorporate smaller ICS (e.g. multiple DCSs and PLCs) and may include a range of common ICS components, such as:

- one or more human machine interfaces (HMI)
- servers, workstations and specialized hand-held devices
- network devices (e.g. firewalls, routers, hubs and Wi-Fi access points)

- specialist components that are unique to ICS (e.g. a Historian).

ICS environments can be interconnected with enterprise IT environments and external networks (e.g. suppliers' networks and the Internet). This creates an extended technical architecture, which is typically segregated by the use of demilitarized zones (DMZ).

The relationship between levels in a technical ICS architecture has implications from a security perspective, and the architectural model adopted will influence how ICS environments can be secured.

Complexity, challenges and weaknesses

In today's modern, interconnected world, the potential impact of inadequately securing ICS can be catastrophic, with lives at stake, costs extensive and corporate reputation on the line. As a result, business is under growing pressure to improve and maintain the security of ICS environments.

This pressure is fueled by:

- Regulatory bodies highlight the significant concerns about ICS and cyber risk;
- Cyber attackers becoming increasingly sophisticated and well-resourced;
- The profile and potential for misuse of the equipment (e.g. IoT devices);
- Major and widely publicized cyber security incidents, along with accompanying headline publicity;
- Expanding media coverage of technical ICS security vulnerabilities.

Organizations are therefore faced with a lack of assurance over the security of ICS environments and have serious concerns about the effectiveness of ICS security arrangements. This situation is compounded by an increasing yet unclear level of risk to these environments, and constraints on ICS protection.

Security Status unknown

There are many different types of ICS with varying purposes and levels of criticality, including those used to support complex, critical environments such as a nuclear power plant, a chemical plant, or a manufacturing plant. ICS may also constitute simple process control systems for air conditioning units, elevators or vehicles that are often less critical. Consequently, many organizations are faced with a lack of assurance over the security of increasingly diverse ICS environments.

Unknown extent of security weaknesses in ICS environments

Many organizations have concerns over the extent and severity of information security weaknesses in ICS environments, compounded by: known technical security weaknesses in ICS components; insufficient consideration of security requirements; a

range of sophisticated attackers; and the nature, scale, complexity and costs associated with ICS and the machinery they control.

Inconsistent ICS regulatory landscape

Some ICS environments (particularly those that support critical nuclear environments) are subject to stringent legal, regulatory or contractual requirements, which often extend to providing assurance that security obligations have been met.

However, for many ICS environments, information security requirements and obligations are often inadequate, vague or incomplete, particularly those relating to ICS products and services. Consequently, there can be a lack of assurance regarding ICS information security.

Heavy reliance on ICS suppliers

Many organizations are heavily reliant on specialized products and services from ICS suppliers, who focus on functionality, often at the expense of information security. These external suppliers are seldom managed closely enough, or have sufficient input from security specialists, to ensure that the provision of ICS products and services meet security requirements.

Inherent ICS design weaknesses

ICS and the physical machinery they control are often built using proprietary hardware and software, with little consideration for information security. Consequently, the implementation of many generic enterprise IT security controls may be impractical or unsafe.

Some of the reasons why ICS suffer from security-related design weaknesses are because there is:

- an absence of rigorous regulatory requirements for security in ICS
- a lack of choice for customers looking to acquire secure ICS products and services
- difficulty in upgrading or replacing ICS components
- insufficient pressure on vendors from customers to improve security in ICS products.

ICS security vulnerabilities

Technical security vulnerabilities frequently exist in ICS, including: inherent design failings; inflexible network configuration; system and network monitoring restrictions; and access control weaknesses. Once technical ICS security vulnerabilities have been exploited, ICS components are susceptible to a range of attacks (e.g. session hijacking, malware infection and account takeover).

Larger attack surface due to increased connectivity

ICS are exposed to a much larger attack surface due to increased connectivity, providing attackers with greater opportunities to access and target vulnerable ICS environments. ICS therefore requires a higher level of protection, including security mechanisms such as authentication, encryption and rigorous monitoring.

Targeting by sophisticated attackers

Threats to ICS environments - which are becoming increasingly prevalent and well-resourced - are increasing in number, sophistication and potency. The particular concerns are about adversarial threats to ICS environments, including nation states, hacktivists, organized criminal groups, suppliers, unscrupulous competitors and disgruntled employees.

Safety vs Security

The complexity of ICS environments presents organizations with significant challenges to the way in which they can be secured, a situation often compounded by a lack of formal management oversight, conflicts between safety and security requirements, and the confusing use of terminology.

ICS specialists focus on the safety, reliability and availability of physical machinery, whereas information security specialists concentrate on the confidentiality, availability or integrity of information.

As a result, the information security team often does not fully appreciate that some information security controls cannot be simply transferred from enterprise IT to ICS environments (if at all) without careful tailoring. In contrast, ICS teams may not be aware how:

- ICS network connectivity and use of commodity IT make ICS vulnerable to information security incidents;
- Information security incidents can affect the safety, reliability and availability of ICS and the physical machinery they control;
- Compromised ICS environments can be used to disrupt connected enterprise networks and gain access to corporate or personal information.

Lack of ownership for the protection of ICS environments

Often individuals were not formally appointed to be accountable for the security of:

- individual ICS environments (e.g. an ICS Environment Owner)
- ICS security across the organization (e.g. a high-level, cross-functional steering committee).

Confusing ICS terminology

Terminology relating to ICS components has evolved and common usage can vary between teams, organizations, industry sectors and ICS suppliers.

Thus, when determining how to improve the security of ICS, terminology can remain an obstacle as assumptions are made about the meanings of even basic terms.

A common example is that the word ‘availability’ means different things to ICS, information security and IT specialists.

Inadequate knowledge of how to implement ICS security controls

When securing ICS environments, information security specialists frequently find themselves operating in unfamiliar territory. Consequently, they may not be equipped with sufficient training, awareness and guidance to:

- Adequately understand ICS environments;
- Acknowledge the security limitations caused by ICS safety requirements;
- Know what to do to secure ICS or how to do it;
- Develop the skills and resources to secure ICS.

Technical vulnerabilities

In addition to mainstream technical vulnerabilities, ICS environments are susceptible to technical vulnerabilities that are more specific to ICS. There are four main types of specific technical ICS vulnerability, which relate to:

- Inherent design failings;
- Restrictive network requirements;
- System and network monitoring restrictions;
- Access control weaknesses.

Inherent design failings

ICS components – particularly proprietary and legacy components – often have inherent weaknesses (typically once network connected), because they:

- Run out-of-date, sometimes unsupported software, such as Windows NT, XP or CE;
- Cannot be patched easily and, where they can be patched, they can require a complete reimage, rather than a simple patch;
- Are not designed to accommodate frequent and timely updates (e.g. an organization needs to wait for scheduled maintenance or can only apply updates using portable storage devices);
- Are usually bespoke (e.g. one nuclear plant can be different to another nuclear plant – even if using the same ICS components), meaning that software updates may still require local validation;
- Are provided with security weaknesses by ICS suppliers (e.g. due to inadequate supplier vulnerability management procedures);

- Are not able to run many types of security software (e.g. malware protection or intrusion detection software) due to unacceptable impact on real-time performance
- Do not integrate well with security tools;
- Cannot be easily reconfigured for use in an ICS security architecture.

Restrictive network requirements

Some ICS components are dependent on critical IT services (e.g. DNS, databases and email). The degree of dependency is often unclear and segregating ICS components can cause unexpected or adverse activity in ICS environments. For example, dependence may be undocumented, which could result in network segmentation that affects the safety, reliability and availability of ICS and the physical machinery they control.

Due to the unique nature of ICS environments, mainstream network devices (including routers, firewalls, IDSs and encryption devices) often need to be configured differently to those deployed in a conventional enterprise network (e.g. filtering, blocking and allowing different types of network traffic). For example, ICS environments will often need to be configured to ‘fail safe’, as opposed to ‘fail secure’, to minimize operational disruption and maintain safety in a failure situation. In these situations the security of ICS will, in part, depend on rigorous security monitoring to detect adversarial threat events.

System and network monitoring restrictions

ICS can use monitoring technologies, such as the SNMP, which is a common protocol enabled on enterprise networks to perform system and network management tasks on network devices. However, ICS environments often make use of outdated, legacy protocols such as SNMPv1 that are vulnerable to attack (e.g. eavesdropping on traffic and relay attacks). Many ICS components provide limited or no event logging capability. Where event logging is possible, enabling it could have significant implications for CPU, memory and disk resource, which could affect the time-critical operations of ICS components. An intrusion prevention system (IPS) may be used on an enterprise network to analyze and automatically block or filter particular network traffic. However, deploying them in ICS environments could compromise communications that affect the safety, reliability and availability of ICS and the physical machinery they control. As a result, an IDS combined with manual intervention should be considered to help ensure legitimate ICS network traffic is not affected. The use of automated vulnerability scanning tools is popular on enterprise networks but can cause unexpected or adverse activity when deployed in ICS environments. Security scanning tools that are active (as opposed to passive) connect to, and interact with, devices on a network. Using this type of scanning tool in ICS environments could affect network performance, cause unexpected behavior in ICS components, or cause them to fail or become unstable.

Access control weaknesses

Some ICS components require user accounts to have special access privileges (e.g. ‘root’ in UNIX systems or ‘Administrator’ in Windows systems) to function correctly. Removing or disabling these privileges could stop the ICS component functioning, adversely affecting the safety, reliability and availability of ICS and the physical machinery they control. Restricting logical and physical access in ICS environments is often not possible. It is common in ICS environments for user accounts and passwords to be shared by more than one individual, preventing the ability to provide accountability for a single individual’s action.

Shared credentials are often required for:

- An automated operational log in a control room that is in continuous use by all individuals on a particular shift, who need to make frequent log entries, without individual authentication;
- Maintenance operators using identical PLCs in a factory (which are unlikely to support an identity store like Active Directory) who could not perform their duties in a timely manner if hundreds of different accounts and passwords were required;
- Safety-critical actions that must be performed immediately (e.g. an emergency stop to shut down a dangerous operation), thereby overriding requirements for conventional identification, authentication and authorization.

Examples of ICS accidental threats

Like corporate environments, ICS environments are not immune from the effects of accidental threats. These types of threat often relate to the actions and behavior of individuals working in ICS environments, such as ICS operators and engineers, who can be a weak link in the protection of ICS environments. Operators and engineers working in ICS environments may not have received sufficient training and education in information security or be able to perform basic tasks that prevent accidents from occurring.

Technology convergence and interconnectivity exposes ICS to an increased number of potential accidental threat events. While they are almost never publicly reported, these events can include:

- Connecting an ICS to ‘the wrong network’ (e.g. an enterprise network or the Internet);
- Connecting personal devices to ICS networks (e.g. using ICS Wi-Fi networks for personal mobile devices and laptops);
- Using a portable storage device, such as a USB stick, that may contain malware;
- Misusing ICS devices (e.g. installing and playing games on a supervisory station), which wastes processing resources and increases the attack surface;

- Upgrading or configuring a software package before the change has been tested and approved for installation in the ICS environment.

Employees and suppliers may not realize the interdependencies between different systems and unintentionally disrupt ICS operations when performing activities on technical infrastructure in seemingly unrelated parts of the organization.

Threat actors

To protect ICS environments it is important to understand, identify and profile the main threats exposed related to ICS environments. Threat profiling involves identifying the threats to the organization and examining the range of threat events they can initiate against ICS environments.

Nation states and organized criminal groups

Nation states are interested in how they can influence or disrupt other nation state governments, commercial businesses and organizations that are part of a country's critical national infrastructure (CNI). The ability to target ICS over the Internet has increased that interest. In 2017, the US-CERT issued an advisory about an 'advanced persistent threat' targeting critical infrastructure by a group called Dragonfly, who are reported in the press as being a nation state.

Example: Stuxnet, severe disruption to nuclear fuel production

In mid-2010, security experts from VirusBlokAda, Kaspersky and Symantec, as well as journalist Brian Krebs, reported on the malware Stuxnet which had infected centrifuges in several Iranian nuclear facilities including the Natanz plant. The malware spread out of its intended target, infecting PLCs in industrial facilities located in other countries, including Indonesia and India. The Stuxnet malware:

- Was targeted at specific computers running Siemens software;
- Produced fake industrial process control signals so that abnormal PLC behaviour would not be detected;
- Was highly sophisticated, using numerous zero-day exploits to spread across its intended targets.

Hacking groups and individual hackers

For some time, security researchers and hackers have published major security weaknesses relating to ICS at security conferences including DEFCON25 in 2017, Black Hat in 2014 and the OverDrive Hacking Conference in 2017. At Chaos Computer Club in 2015, the SCADA StrangeLove team presented the results of their research on railway systems' security. Developed over three years in cooperation with major organizations in the rail sector worldwide, the results indicated that railway systems

are not difficult to hack – even though the task requires specific knowledge of railway automation. The same team later released a list of default passwords associated with ICS from major suppliers. However, not all hackers have such altruistic intentions. Furthermore, by raising awareness, these groups are also reducing the level of skill and effort required to attack ICS, making it more affordable and accessible to an even wider community of hackers.

Example: German blast furnace, physical destruction due to phishing attack

SANS reported that a 2014 incident at a German blast furnace started with a phishing attack on the victim's enterprise network, which was used as an entry point to the ICS. SANS speculated that the furnace suffered a loss of control, could not be shut down and this led to its physical destruction. To illustrate the potential impact, SANS drew a parallel with an explosion at a similar furnace in the UK several years earlier, which although not ICS related, resulted in two fatalities and thirteen injuries.

Employees and suppliers

Employees (including consultants, contractors and employees of external parties) and suppliers represent a threat to ICS due to their unique knowledge, privileged access and susceptibility to social engineering. A recent US-CERT warning about the Dragonfly attacks against critical infrastructure, describes how social engineering attacks against workers are a key stage in the cyber-attack chain. Disgruntled insiders have attacked ICS, such as the Maroochy Water incident, where an ex-contractor gained unauthorized remote access to sewage equipment and caused 800,000 liters of sewage to spill out into local parks and rivers.

Suppliers often place operating manuals, other ICS documentation and details about system updates online. Not only is this a powerful source of information for attackers, it has enabled groups such as nation states and individual hackers to infect these files with malware in order to attack ICS: thus, when engineers or technicians download infected documents, the malware compromises their machine and in turn attacks the ICS.

Common ICS Threat Events

A key part of profiling adversarial threats involves examining the techniques and methods (threat events) that can be used by attackers when targeting ICS environments. Attackers have many techniques at their disposal, therefore organizations need to protect against a range of threat events associated with ICS environments

The table below lists common ICS threat events including a brief definition of the threat event.

ICS Threat	Definition	Additional information:
Scanning of online ICS assets	The threat performs unauthorized scanning or probing of ICS to gather information that could be used to initiate subsequent threat events	Scanning can be performed using different means, such as via automated tools designed for scanning IT systems and internet-based search engines
Unauthorized use of remote ICS control software	The threat obtains unauthorized access to remote ICS control software and uses it to make unauthorized connection to ICS.	Threats can gain unauthorized access to remote access connections (e.g. a virtual private network (VPN)) in different ways, which include: <ul style="list-style-type: none"> • exploiting insecure use of network cryptography • gaining access to legitimate authentication credentials (e.g. due to the use of a weak password) • conducting offline password cracking attacks on a password database • theft or leakage of authentication information, such as tokens • compromising the security of the connection.
Malware disguised as ICS software update	The threat compromises the developer of software (e.g. ICS supplier or internal development team) and infects ICS software with malicious content.	Unsophisticated threats apply techniques to: <ul style="list-style-type: none"> • develop or modify different types of malware (e.g. by using publicly available malware development kits that can incorporate exploits for the most recent, known technical vulnerabilities) • distribute malware (e.g. by using email communications and manipulating applications and systems that connect to ICS). Sophisticated threats can apply more advanced techniques to: <ul style="list-style-type: none"> • develop malware (e.g. producing bespoke and targeted malware using unpublicized or 'zero-day' vulnerabilities) • distribute malware (e.g. targeting key individuals via spear phishing attacks or infecting their portable storage devices (e.g. USB sticks)) • conceal malware (e.g. using rootkits or anti-detection techniques).
Exploitation of ICS connections from less protected software/ business areas	The threat takes advantage of poorly designed network architecture to gain access to, and target, exposed ICS.	Threats can exploit: – unnecessary or unprotected internet connections – weak filtering on internet or internal network connections – a lack of segregation of critical ICS or business functions (e.g. no DMZ in place).
Exploitation of inadequately	The threat takes advantage of dial-up/cellular modem connections that are used to	Threats can access and compromise ICS that are connected to modems by:

protected ICS modems	support or maintain ICS, or to gain access to ICS.	<ul style="list-style-type: none"> gaining access to modems and multiplex devices using stolen authentication credentials manipulating telephone systems to bypass modem access control.
Generic and targeted phishing	The threat counterfeits or imitates communications from a legitimate/trustworthy source to mislead recipients into installing malware or revealing sensitive ICS related information (such as usernames and passwords, ICS identification details, technical infrastructure and location of ICS) that can help them gain unauthorized access to ICS.	<p>Unsophisticated threats can apply techniques, such as:</p> <ul style="list-style-type: none"> using generic, publicly available phishing development tools employing high-volume delivery mechanisms (e.g. spam emailing tools) targeting individuals or organizations (e.g. using basic social engineering attacks). <p>Sophisticated threats can apply more advanced techniques that are associated with spear phishing, such as:</p> <ul style="list-style-type: none"> using customized phishing tools targeting specific network shares and repositories of information adopting advanced delivery mechanisms (e.g. counterfeit websites with certificates that appear genuine) performing research to target specific individuals (e.g. ICS operators or engineers, and other individuals with privileged access).
Exploitation of ICS software or web connections	The threat exploits coding bugs or design flaws in software to gain unauthorized access to ICS (e.g. by executing code or in a web browser used to access ICS or modifying the URL sent directly to an ICS-based web server).	<p>There are many different types of software attack that can affect ICS environments by exploiting vulnerabilities, such as inputting bad data into applications, causing buffer overflows, exploiting format string vulnerabilities or session tokens, injecting SQL/LDAP commands, performing cross-site scripting (XSS) or URL forgeries, and forcing remote file inclusion.</p> <p>Threats can target ICS by exploiting vulnerabilities in ICS-related servers, which are used to access and support:</p> <ul style="list-style-type: none"> applications (e.g. end-user applications) services (e.g. web servers, database management systems) operating systems (e.g. Microsoft Windows, Linux, Apple OS X or IBM z/OS) virtual systems (e.g. virtual servers and virtual desktops) networking equipment (e.g. routers, wireless access points and firewalls) ICS (e.g. PLC, DCS and SCADA). <p>Threats can use:</p>

		<ul style="list-style-type: none"> publicly available tools to attack the ICS environment bespoke attack tools to create exploits for unpublicized vulnerabilities (often referred to as 'zero-day' vulnerabilities), for which there are unlikely to be patches available insiders to perform unauthorized actions (e.g. loading malicious dynamic link libraries (DLLs) to cause a buffer overflow).
Compromise of ICS supplier or business partner	The threat compromises an ICS supplier or business partner of the organization to gain access to related ICS.	Threats can use compromised ICS suppliers and business partners to: – modify the design, manufacture or distribution of critical ICS components at selected suppliers to replace those (that the organization requires) with modified or corrupted components – 'pivot' off compromised systems to gain access to the organization's ICS environment.
Infection of ICS supplier website and software with Trojan-based update installers	The threat compromises ICS suppliers and infects their support systems with Trojan-based malware affecting ICS software. ICS software with infected update installers is subsequently downloaded and installed by the organization.	Threats with access to ICS supplier systems can modify source code, configuration settings and dynamic link libraries (DLLs). Threats embed ICS software with Trojan code and make the software available for download by the organization (an attack technique referred to as water-holing).
Gain access to enterprise IT and other ICS support systems	The threat obtains access to authentication credentials for enterprise IT systems and uses them to gain and maintain unauthorized access to ICS-related systems	Threats can obtain authentication credentials in different ways, such as by: – causing a leak of authentication details (e.g. convincing individuals to reveal passwords on social media platforms) – exploiting insecure storage of authentication information (e.g. passwords stored in clear text files on mobile devices and USB sticks) – conducting dictionary or brute force attacks on passwords or password databases used to authenticate users on ICS.
Enumerating ICS	The threat uses authentication credentials gathered (e.g. through a successful spear phishing attack) to identify and map network drives, and to collect configuration details about ICS, enabling attackers to traverse compromised networks	<p>Unsophisticated threats apply techniques to discover and gather user credentials, such as:</p> <ul style="list-style-type: none"> using generic, publicly available enumeration tools targeting all discovered network shares. <p>Sophisticated threats can apply more advanced techniques, such as:</p> <ul style="list-style-type: none"> developing bespoke enumeration tools targeting specific network shares, repositories of information and proprietary ICS.
Exploit insecure features of ICS technology	The threat exploits insecure features of ICS technology to install malware or alter the configuration of the ICS.	<p>Threats can exploit ICS technology used for monitoring and control across multiple ICS environments.</p> <p>Exploit techniques can include:</p>

		<ul style="list-style-type: none"> • manipulating debug capabilities in ICS firmware or software to install malicious code • modifying ICS network technology (e.g. wireless-based sensor networks) to affect the measurement of temperature, flow, pressure and humidity.
Generating false ICS network traffic	The threat generates or replays ICS network communications to create false network traffic and conceal malicious activity.	Threats can intercept and modify network traffic (e.g. transmitted to and from the HMI) in real time using custom tools or more advanced attack techniques (e.g. by performing cryptanalysis of strongly encrypted communication sessions).
Interception and modification of ICS communications	The threat gains unauthorized access to ICS-related network traffic to: <ul style="list-style-type: none"> – observe ICS-related information transmitted across ICS networks (i.e. sniffing) – modify ICS network traffic during transmission (i.e. spoofing) – disrupt the network or masquerade as a legitimate ICS on the network. 	Threats can perform real-time attacks, such as: <ul style="list-style-type: none"> • intercepting ICS network traffic by executing DNS hijacking or man-in-the-middle attacks and exploiting poorly encrypted or unencrypted communications • modifying network traffic in real time using custom tools or other more advanced techniques (e.g. by anticipating TCP/IP packets sequences and performing cryptanalysis of strongly encrypted communication sessions)
Disrupt or disable ICS	The threat impairs the availability or performance of ICS by exploiting technical vulnerabilities in the HMI	Threats can interfere with wireless communications (e.g. Wi-Fi or GSM/CDMA) to impede or prevent communications from reaching intended recipients. Threats can: <ul style="list-style-type: none"> • use publicly available and bespoke network traffic manipulation tools • exploit single hosts in multiple ICS locations – adapt to available levels of network bandwidth.
Exploiting vulnerable authentication mechanisms in ICS	The threat exploits technical vulnerabilities in the authentication mechanisms of ICS to gain access to sensitive functions and information.	Threats can overcome the authentication mechanisms in ICS by: <ul style="list-style-type: none"> • bypassing authorization checks • executing privilege escalation attacks • performing forced browsing/navigation.
Distributing ICS ransomware	The threat distributes ransomware to specifically target the organization's ICS	Threats can interfere with wireless communications (e.g. Wi-Fi or GSM/CDMA) to impede or prevent communications from reaching intended recipients. Unsophisticated threats apply techniques, such as: <ul style="list-style-type: none"> • developing or modifying ransomware using publicly available ransomware development kits that can incorporate exploits for the most recent, known technical vulnerabilities

		<ul style="list-style-type: none"> • distributing ransomware through the use of portable storage devices (e.g. USB sticks) or by using email communications and manipulating applications and collaboration platforms that connect to ICS. <p>Sophisticated threats can apply more advanced techniques, such as:</p> <ul style="list-style-type: none"> • developing ransomware (e.g. producing bespoke malware using unpublicized, or 'zero-day' vulnerabilities) • distributing ransomware (e.g. targeting key individuals via USB keys or infecting portable devices they may use) • concealing ransomware (e.g. using rootkits or anti-detection techniques).
Exploiting ICS protocols	The threat exploits weaknesses in technical protocols used by ICS to take unauthorized control of ICS components.	Threats can manipulate ICS protocols to control specific makes and models of ICS components or it can be repurposed to attack any ICS using particular communication protocols and components.

The fundamental ICS controls

There is no established recipe for how to design security in nuclear ICS, but there are a number of accepted work practices that every nuclear organization should implement. This section lists recommendations that are helpful to achieve a good security culture and systematic security work with the ICS. Some recommendations are technical in nature and others focus more on methodology.

Commitment and responsibility for security in ICS

Management is responsible for running the company's operations in a business-like manner and it is not always certain that the security of ICS receives the attention it requires. One reason could be difficulties in seeing how security investments in the short-term contribute to business performance. It can be especially difficult to address those specific information security-related aspects prevalent in the ICS. For many, information security only relates to the administrative systems.

In order to motivate management to understand and highlight these issues, a sustained educational initiative is required. It is important to respect the fact that security work is often perceived as something boring and tedious. It is therefore important to explain how a heightened level of information security in the ICS improves the business.

A first step can be to try to make time for a short presentation during a management team meeting. It is important to be well prepared before such a meeting. Avoid scaremongering. Instead describe the way in which the business can become more

efficient by managing risks at an early stage. When you discuss risks, try to make the risks concrete and describe how they can be remedied and thus improve the business. Also prepare a tangible and relatively simple proposal for what the next step might be – for example, a risk analysis of a defined part of the ICS.

An important goal is to ensure that the ICS are taken into consideration in the organization's information security management system (ISMS). If there is no ISMS in the operations, the first step is then to have management assign someone the task of developing such a system.

Other recommendations in this guide contain proposals for elements that should be considered in the organization's systematic information security work in respect of the ICS.

Recommendations:

- Work with long-term objectives and try to get management themselves to show an interest in security work and the benefits it can yield for the business.
- Try to describe what different measures cost – both in investment and in working hours.
- Relate the cost to the benefit that the measures yield for the business.
- Propose tangible changes in the organization's steering documents with the goal of having the ICS considered in the systematic information security work.
- Avoid talking about technology and instead focus on how long-term efficiency can be improved concurrently with increased security work in the ICS.
- Use specific examples applicable to the operations in question in order to explain what IT security in the ICS entails.

Clarify roles and responsibilities for security in ICS

In many organizations, process-oriented control is common when it comes to administrative information systems. In this management model, there are often designated system owners, information owners, administrative managers, operations managers, system administrators or similar positions.

For information and control systems, this allocation of roles and responsibilities is often non-existent. At times, vendor representatives are the closest thing to an IT technician or system administrator available. Moreover, practical administration of the systems may be handled by process engineers, whose main area of expertise lies outside of logical security in information and control systems. This leads to an organization having insufficient or no knowledge of the IT properties of the ICS. Subsequently, there is reduced control and ability to manage how the technology is used.

Recommendations:

- Create an information security policy for ICS. The allocation of responsibilities for security issues is most easily clarified in this way. The policy can either be a

separate document, which must then be related to the organization's other steering documents, or the issue may be resolved through supplements to the organization's information security policy.

- Coordinate the allocation of roles and responsibilities in respect of the administrative information systems and the ICS. It should be clear which systems are managed by the organization's central IT support and which systems are managed locally at the production location.
- Let the organization's central IT support be responsible for the overall integration and create a coherent approach to the security issues even though some systems are managed locally.
- Clearly document the requirements imposed on a system owner.

Maintain processes for system surveys and risk management in ICS

To maintain proper security in ICS, it is important that there is a process to survey and understand the operation's information flows, information assets and system dependencies. That is, the relationship that exists between the activities and the different types of systems.

Analyzing the operation's processes, systems and information requires a deep understanding of the consequences that a faulty or disrupted function may involve, both for the physical process and for the organization. This is an important prerequisite for creating a relevant risk evaluation and a classification of which systems are most critical and which information is most critical.

An organizational and system survey should result in lists of access and connection possibilities, system classifications and operational priority classifications. There should be diagrams of the ICS which are detailed enough to make critical components and systems identifiable. A system diagram shall, for example, contain IP addresses, communications protocol, version number, information on the operating system of computer resources, technical information about local devices such as PLCs, and so on. It is also helpful if each component in the system diagram has a unique serial number that points to an entry in a configuration database. In order to establish the electronic security perimeter, all connections to industrial information and control systems must be identified. In addition to the Intranet, this includes, for example, remote connections to business partners, vendors and the Internet. Note that all wireless connections should be treated as remote points. Connections to the organization's administrative information system (Intranet) should be considered external connections.

Recommendations:

- Take an inventory of the organization's assets and identify those that are critical by applying a risk-based approach. Then identify the critical cyber assets.
- Establish a documented process for how risk analyses are carried out and the conditions under which they are updated. Select a risk analysis method based

on purpose of the analysis and the information available. The choice of method should take into account the ability to easily update the risk analysis.

- Maintain a configuration database to facilitate the search for various components and parameters in a complicated network topology.

Ensure systematic change management in ICS

Systematic management of changes and versions of parameter configurations, settings and data files or programs is important in order to prevent disruptions, unnecessary troubleshooting or serious problems in ICS. Systems and applications that organizations will use for a long period of time, such as in industrial processes, entail special requirements for strict control of change management. In the ICS, it is important that all involved parties – vendors, system administrators and users – have a correct and common understanding of the system's current configuration and operational status. Separate testing, development and operating environments are common for administrative information systems. Unfortunately, this is not the case for ICS, which makes it even more important to allocate sufficient resources to systematic change management in these systems. There should be a formal process that specifies how to obtain authorization to make changes in ICS. This should also apply to temporary changes and changes to support equipment. Everything that is not explicitly authorized should be forbidden.

Recommendations:

- Upgrade software incrementally. Preferably in consultation with system vendors, due to legal and technical requirements.
- Ensure that the formal process for change management includes:
 - a description of what is subject to authorization requirements,
 - a procedure for obtaining authorization to make changes,
 - a description of how tests before and after a change are to be conducted (including a description of the changes that require testing in a separate test environment),
 - requirements for how documentation shall be updated after changes
 - and requirements for how personnel shall be informed of changes (for example, in which cases special operator training is required).
- Ensure that rules and procedures related to changes in the ICS are in keeping with existing change rules in physical processes or facilities.
- Inspect tools (computers/laptops) used for updates of settings and programs.
- Check the management of the hardware and software tools, such as compilers and file transfer methods, used in the change process.
- Check devices so that only known and verified system software (firmware) is used.
- Perform differential checks against previous versions before and after all updates.

Ensure systematic contingency planning and incident management in ICS

To ensure the organization's ability to survive serious disturbances, there must be contingency planning that includes clear descriptions of routines, roles and responsibilities during emergencies. Examples of such disturbances are power outages, control system failures and key operating personnel out on sick leave.

In addition to continually following up and updating contingency plans, it is vital for personnel to participate in preparedness training exercises and for operations to be regularly tested to ensure satisfactory functionality in the event of an emergency. For ICS, it is often the case that the restoration of the system must happen quickly, and tolerance for error is minimal. It is therefore particularly important to ensure backups for these systems.

All unexpected events (incidents) that lead to a disturbance in the ICS, such as a service becoming unavailable or having reduced functionality, must be documented for later analysis. One of the difficulties with incident management is finding a balanced structure for how incidents can be caught and reported without this being perceived as obstructive to the normal work process. It is also important to motivate the organization by communicating the purpose behind reporting incidents and providing information on the results of incident management. Without this communication, it can be difficult to maintain motivation to report incidents and vulnerabilities.

Recommendations:

- Establish and maintain incident management procedures and contingency plans for the ICS.
- Analyze incidents to determine and understand the problem of origin, the extent (spread), and the direct and indirect consequences. Check, for example, if it is a case of simple errors and whether they occurred due to intentional or unintentional events.
- Ensure that the following items are included in the contingency planning:
- routines for handling operations manually (run the process without computer support)
- routines for restoring both data and configuration settings as well as restarting the process
- contact details for system owners, operators, service technicians, other personnel, vendors and support
- description of support agreements and suspension times
- description of how central control system components can be replaced
- description of how and from where emergency operations are to be conducted if the disturbance is serious.

Introduce security requirements in ICS right from the start in all planning and procurement

Since it is difficult and expensive to achieve an acceptable level of security in ICS after implementation, security requirements should be included from the very beginning in system specifications and needs analyses. Because many system solutions are fully or partially procured from external parties, special attention must be given to security issues during procurement work.

Security in ICS should be expressly addressed in procurement documentation, testing and handover management, contracts and steering documents for maintenance or operation tasks. Procurement can encompass both new installations and complete or partial modernization of existing solutions. Security requirements should be incorporated as an important element in all vendor agreements, including service and maintenance agreements.

When modifying ICS, special consideration must be given to IT security matters since the changes will most likely affect the existing information and control system in a manner that the original designers had not considered. For example, in older information and control systems there was often a presumption that access to equipment would only be possible via local physical presence. Nowadays, physical separation is no longer always possible which places high demands on a logical separation between different parts of the ICS.

Recommendations:

- Use threat and risk analyses as well as various surveys to gather requirements.
- Follow up that vendors satisfy detailed requirements for security and protective functions in systems and applications.
- Require the vendors to present their methods and processes (such as internal developer handbooks) used to guarantee the quality of their own security work.
- Be sure that vendors receiving information on the ICS sign non-disclosure and security agreements.
- Include requirements for deployed equipment to be tested in a secure manner. A control computer, for example, must be able to cope with the volume of traffic that occurs during a penetration test.
- Ensure that there are documented procedures for how security aspects should be taken into account during procurement.
- Conduct regular audits to ensure compliance.

Create a good security culture and heighten awareness of the need for security in ICS

It is important to establish the understanding that security in ICS is a mission-critical issue. It takes long-term efforts to influence understanding and attitudes and the commitment of executive management is extremely important, as always when it comes to security matters. The importance of this commitment is in part because

security in ICS requires increased resources and because it requires collaboration between parts of the organization that do not normally work together.

In order to achieve a high level of security in ICS, it is necessary to have knowledge of traditional IT security, control systems and the underlying process. Security work therefore requires collaboration and trust between individuals from different cultures with different security traditions and organizational seats. This requires regular education and training of both IT personnel and control system operators. It is also important to allocate time and resources so that different parts of the organization can meet and exchange experiences.

ICS are included in system solutions that have very long service lives. It is particularly important to try to imagine how the systems will be used or potentially misused in the future. Ignorance or unclear routines can cause many normal activities to lead to potential security problems.

Recommendations:

- Establish an administrative security program to create a general approach to IT. This provides a good level of security awareness, encourages critical thinking and creates a positive attitude towards working with issues that improve security.
- Before a person is allowed access to the ICS, he or she must undergo appropriate training. It is important that management understands the importance of training, allocates sufficient resources and continually revises the organization's program for in-service training.

Work with a security architecture in the ICS

Working with a security architecture implies a structured and systematic approach to organizing the protection and defense mechanisms of the organization. The security architecture is based on a number of governing security principles with the aim of protecting information with regard to confidentiality, correctness, availability, and traceability. An important part of the security architecture is to maintain "defense in depth". Defense in depth consists of overlapping security mechanisms installed at several different levels in the network or in different systems and applications. The security mechanisms are sometimes redundant, e.g. multiple firewalls, and sometimes complementary, e.g. combinations of intrusion detection systems, firewalls, encryption of network traffic and data, authentication mechanisms and the logging of use and abuse. Different security mechanisms can constitute boundaries in a zone model, where different zones represent groupings of components and systems with different security or functional criteria. In zone boundaries, a toggle system or a data diode, for example, can function as adequate protection in the event information is only permitted to be transported in one direction. A file gateway is another mechanism that can be used in a zone boundary. A data lock performs a more detailed and controlled examination of the data to be passed. The communication within an information and

control system may also need to be protected. Communication between field equipment such as PLCs and local systems is usually based on industrial protocols with little or no security. Zone models should also be considered at this level.

Recommendations:

- Design security architectures for ICS that include principles and security concepts for
 - network security;
 - system security;
 - application security;
 - operational security issues.
- Divide the ICS into different zones with security levels adapted to how critical the systems are.
- Depending on system and information classification, among other things, so-called sub-zones may also need to be created.
- Divide up the network based on functional classification.
- Data traffic across zone boundaries should be handled with additional restriction and should also be monitored and logged. For certain types of IT environments, it may be useful to use a toggle-system, data diodes and file gateways.
- Introduce functions for monitoring, alarming, traceability logs, network recording and analysis in zone boundaries.
- Avoid connecting IT systems and their support functions (e.g. data storage) to multiple zones in parallel, as this short-circuits the zone division and actively counteracts the zone model as a security concept.
- Place insecure services and other external connections in the demilitarized zone (DMZ).
- Create an electronic security perimeter (logical perimeter) around the ICS. Note that the administrative systems are outside this security perimeter.
- The network architecture should be segmented with overlapping security mechanisms.
- Feel free to use different communications protocols between different parts of the network. If one protocol is used between the control system and a DMZ, another protocol should then be used for further communication between the DMZ and the organization's administrative information systems.

Continuously monitor connections and systems in order to detect intrusion attempts in ICS

In addition to horizon scanning, monitoring of incidents and updating of risk analyses, the organization needs to continuously monitor and detect intrusion attempts. Monitoring of own systems and their communications, combined with horizon scanning, provides a better understanding of current threats, changing attack trends and current malicious code. This monitoring should be performed both internally, within

the organization's own systems, and externally to monitor attacks against external connections.

There are primarily two types of intrusion detection systems (IDS). Some systems recognize attack attempts via analysis of communication flows – so-called network-based intrusion detection systems (NIDS). Others monitor events in a computer system or usage patterns in an application – so-called host-based intrusion detection system (HIDS).

An advanced variant of these systems are so-called intrusion prevention systems (IPS), which can also work to deflect attacks.

Note that use of IPS in ICS with incorrect attack classification can lead to legitimate traffic being blocked (so-called false positives). A security system that unpredictably blocks control commands or result codes is unacceptable in ICS.

So-called honey pots can also be used as a complement to indicate attack attempts in progress. Honey pots are often targeted to also collect information about an attacker or intruder. A simple solution that can be suitable in ICS is to install a computer in the network that does not normally receive any traffic and that triggers an alarm if this occurs (such honey pots are sometimes called canaries or honey traps). Even an attempt to communicate with this computer can be reason to suspect that an attack attempt is in progress or that an attacker is attempting to prepare for an attack by surveying the network.

Recommendations:

- Continuously monitor external connections and internal systems to detect all forms of intrusion attempts.
- Continuously analyze logs and tracing data from intrusion detection systems.
- Establish long-term storage for logs and tracing data from intrusion detection systems. This data is needed if further investigation is initiated, which can occur long after the initial problem surfaced.
- There should be a role responsible for honing in on any warnings from the technical systems.

Conduct regular risk analyses of ICS

One of the security organization's most important activities is to regularly update and evaluate the risk analyses that have been conducted. A risk analysis is the most important input for making decisions on which measures should be taken to prevent operational disturbances, loss of production or even human injury and environmental damage.

The basic presumption that should be applied to all IT system risk assessment is that the enemy is familiar with the system. When it comes to information and control systems, many unfortunately assume the opposite – that no outsider knows the details

of the vendor-specific solutions. This is sometimes referred to as security by obscurity, which seldom succeeds since the attacker has a wealth of choices when it comes to factors such as method and time of attack. Vendor-specific communications protocols, encryption solutions or operating systems therefore do not in any way guarantee security. The results are more often the opposite – they cannot stand up to open examination by researchers or technical specialists.

It is also important that risk analyses are carried out before introducing changes in an organization. Since ICS may have internal dependencies that are not always obvious, one should critically analyze the potential indirect effects of changes.

There are also risks that come to light without a formal risk analysis having been performed. It is important that there are processes to capture these risks and manage them according to their assessed level of seriousness.

Recommendations:

- Conduct risk analyses of ICS. A risk analysis can be conducted for a defined subsystem, or for a more general operation.
- Update the risk analyses in accordance with the methods that have been previously established and documented. The choice of risk analysis method to be used in the particular case depends on the purpose of the analysis and the information that is available on the system in question and its potential threats.
- Remember to update the system survey (system diagrams, configuration databases and the like) while updating the risk analysis, where necessary.
- Based on the operational analysis, there should be defined which systems and information resources that are mission-critical.
- The risk analysis shall be documented in a pre-defined manner and approved by management. The documentation should, at a minimum, include detected vulnerabilities and assessment of risks, as well as descriptions and prioritization of possible countermeasures.
- The following information may be required to perform a risk analysis: Incident and interference data (logs and material from horizon scanning), results from conducted security audits (security tests and administrative audits) and checklists.

Conduct periodic technical security audits of ICS

Conducting practical security audits and technical controls makes it possible to create a more realistic picture of security in systems and installed functions. There are some important differences between practical security tests on administrative IT systems and the IT equipment used in ICS which often have poor security qualities (for example, field equipment such as PLCs and RTUs). The equipment can often be disrupted or attacked due to trivial programming errors. Unfortunately, it is not uncommon for this to result in a crash, restart or faulty behavior of the test unit in response to a simple security test.

In some cases, the only installation that exists is the one in production and there is no test or development environment that can be used for practical security tests. Careful planning should precede a practical security test of ICS, including a run-through of how any disturbances resulting from the test are to be handled. The test plan should be approved by the organization's management. The basic principle is to rely on simple basic methods and interviews of relevant personnel rather than automatic tools for penetration testing of traditional IT systems. Few IT consultants have sufficient knowledge of how to test ICS. Many production environments are highly specialized, which requires an understanding of technologies other than those that exist in IP-based networks. For this reason, it can also be a good idea to have a discussion with system vendors prior to a security test.

When it comes to surveying information and control systems to identify host computers, nodes and networks, traditional methods such as "ping sweep" could disrupt with the system. However, inventorying the control system is an extremely important step of the test process. Instead of using automatic tools, the process often involves carefully examining the documentation and even visiting the actual site of the process and studying physical connections and computers.

When inventorying services and vulnerabilities of various services, active scanning methods (such as port scanning and vulnerability scanning with tools such as Nmap and Nessus) should be avoided in a production system that is in operation.

Recommendations:

- Conduct periodic technical security audits of ICS and connected networks.
- Practical tests can negatively impact control systems and processes. These should therefore only be performed after careful preparation and once the possible consequences of the tests are understood. Instead, use passive methods and manually examine, for example, how routers are configured.
- If active tests are to be performed, then conduct these in a separate test system or in a control system that is not in operation.
- Continuous intelligence analysis should be carried out in order to acquire knowledge on discovered vulnerabilities that could affect the organization's information and control systems.

Continually evaluate the physical security of ICS

ICS, particularly central facilities, have historically had substantial physical protection and in many sectors there are established requirements for how important facilities are to be classified and physically protected.

ICS are often geographically dispersed (decentralized), which makes it more difficult to maintain good physical protection at the remote facilities. Attacks on ICS can be made from equipment in the field. Local units such as PLCs and RTUs can be very sophisticated. For example, a modern RTU can include a web server and more modern

communication methods (Bluetooth, Ethernet port or WLAN) and should therefore have sufficient physical protection. Cables and cross-connection spaces should be located in a manner that prevents unauthorized individuals from physically accessing them and connecting to the network.

Physical access to a system component makes it much easier to gain logical access to ICS. Logical and physical security perimeters must therefore be strictly followed. Keep in mind that certain industries may have their own rules and requirements.

Recommendations:

- Physical protection should be conducted in several ways – the defense in depth principle also applies here – and should include, amongst other things:
- protection of sensitive premises – physical perimeter protection, protection against unauthorized entrance, burglar alarm, camera surveillance and monitoring, fire protection and so on
- authorization control – ensure that only authorized individuals have access to sensitive information and important operating premises
- traceability that applies to individuals and assets – ensure that both individuals and equipment remain in appropriate areas – for example, portable equipment such as laptops for PLC programming should not be left unsupervised
- cables for communication – minimize the risk of cables and cross-connection spaces being subjected to interception or manipulation
- checks of environmental factors – such as ventilation and power supply.
- Establish a good level of physical protection in all facilities and spaces. Balance the physical and logical protections so that they are harmonized. Good physical security without corresponding efforts made with logical security, or vice versa, can undermine the work that has been done.

Regularly ensure that any and all connections to ICS are secure and relevant

ICS have traditionally been physically isolated with few or no communications connections to the outside world. New business needs and efficiency improvement measures have resulted in streamlining solutions with integration between the information and control systems and the administrative systems. All types of connections must be identified and equipped with security mechanisms that are adapted to the organization's security requirements and to the operational requirements set for the various control systems.

Connections to ICS can consist of dial-up modems or ISDN, landline and wireless network connections or Internet-based connections. Examples of network connections are:

- service inputs for vendor representatives
- connection capabilities for on-call personnel who need quick access to the industrial information and control system

- connection capabilities for remote operation of facilities
- connection capabilities for remote reading of sensors in facilities
- connection capabilities for access to supplementary functionality or peripheral systems in facilities, such as camera surveillance, alarm systems, card and access security, fire alarms, etc.

Recommendations:

- Regularly ensure that only relevant connections to the ICS exist, and that these are sufficiently secure.
- Eliminate unnecessary connections. All existing connections are to be formally sanctioned by an authorized manager.
- Disable all unused data ports (e.g. switch ports or USB ports) at the lowest possible operating system level, preferably BIOS level.
- Disable additionally, all unused ports with a dummy connector plug which requires a tool for removal.
- Prevent uncontrolled external or unmanaged hosts connection to the ICS network segments.
- Prevent connecting untrusted removable media (including all types of Mobile Devices like Smartphones, Tablets) on the network or hosts.
- Remote access for vendors or access for on-call personnel requires special supervision. To establish an acceptable level of security, combinations of various methods should be used, such as callback, limitation of connection time, stricter authentication and limitations on which communication methods can be used and which computers can use them.
- All user and system accounts should only have necessary authorizations. Access to files, applications and system resources should be denied if they are not explicitly permitted. All accounts should be equipped with fortified authentication.

Harden and upgrade ICS in collaboration with system vendors

Hardening of computer solutions, system components and applications entails the removal of unused, unnecessary or unknown components of software and configuration and installation of security upgrades (patches). This limits the size of the attack surface and reduces risk exposure. Hardening is a standard measure when it comes to improving security in traditional IT systems. The goal is to always use the most secure variant of system configuration and settings. It is important for hardening to be done in accordance with the change management process that has been established. The attack surface of a system can be reduced by, for example:

- changing factory settings, such as changing default passwords
- choosing more secure alternatives and settings in applications, network functions or operating systems

- deactivating unused functions in applications, network functions or operating systems
- blocking login capabilities for users who are no longer to have access to systems, or limiting users' login capabilities and rights
- correcting known security problems through upgrades (patches).

Hardening and manually closing security holes in system equipment, applications and operating systems – which security documents for ICS sometimes mention – cannot normally be conducted without strong support from vendors. Changing equipment or software settings (including patching) without collaborating with system and application vendors can lead to operational disturbances, create instabilities in control systems and even have contractual consequences.

Recommendations:

- Harden and upgrade ICS so that they are as secure as possible.
- Maintain system security over time by continuing with the installation of patches, upgrades or similar.
- Make sure to document all changes that are made. It is advisable to log this in a configuration database. These recommendations also apply to all peripheral systems and aids – such as laptops used by support technicians – that are used to maintain and run the function.
- When replacing equipment or subcomponents, all new components should be hardened during installation. All hardening and upgrading should be handled according to procedures for change management.

Conduct training and practice regarding IT incidents in ICS

Developments within IT have meant that many organizations have been able to develop new business models and have found new ways to make work more efficient. Unfortunately, this development also involves new security deficiencies which in turn lead to IT vendors being forced to develop new protection and so on. These constant changes make it important to engage in ongoing in-service training.

IT can constitute both the means and the target of different types of attacks. Industrial information and control systems are no exception. One problem is that many who work with these systems have a lack of experience with regard to IT-related attack scenarios. It is therefore important that the skills, procedures and processes that have been developed are practiced regularly. This applies mainly to the IT-related procedures, processes or process steps that rarely or never occur under normal conditions. With the help of exercises, the skills and experiences needed to be mentally and practically prepared for an incident when it actually occurs can be acquired. To implement a completely untested procedure in critical situations often involves great risks.

Exercises also lead to the improvement of methods, procedures and tools.

Recommendations:

- Ensure that all who have responsibilities within the area have built up a good level of expertise and that, through in-service training, they maintain this level of expertise within their respective subject areas.
- Plan and carry out different types of exercises within the area of IT-related incidents within ICS. As an initial step, exercises can be used as a learning element within incident management where IT is a key feature. When procedures, process steps and expertise are in place, the exercises can instead aim to maintain their skills but also to evaluate and fine-tune procedures, methods, tools and working methods.
- Have a documented strategy for exercise and training activities which is regularly reviewed by management. There should be a role with the responsibility for updating the exercise and training strategy.

Follow up incidents in ICS and monitor external security problems

An important prerequisite in all improvement work is that the organization reports, documents and learns from past incidents and security experiences – both those that occur within the organization and those that occur in other organizations. Experience and incident reports should serve as the basis for risk assessment updates (risk analysis updates). They should also be able to lead to corrective measures and reprioritizing of resource allocation.

In order to detect incidents, there must be continual follow-up and monitoring of the organization's security routines and their status. With this monitoring and follow-up, the organization can better handle threats and detect new security deficiencies – both from its own organization and from others. Attention should also be given to external incidents and events that could impact the organization. Physical incidents can be related to IT incidents. For example, a break-in resulting in a stolen laptop could be part of the information gathering that precedes a digital attack. By keeping the organization updated on incidents and security problems that have been discovered externally, it is easier to maintain good preparedness for fighting new threats and vulnerabilities in ICS.

A problem related to knowledge and analysis is that there is very little open information on past disruptions in ICS. At present, there are few forums and communication channels where information is easily accessible to system and facility owners.

Recommendations:

- Put together a group that regularly meets to discuss incidents and risk problems, and analyses how these might impact the security of the organization's information and control systems.
- The group should consist of representatives from management as well as from both the process control and IT side. It is important to create a culture where

employees are confident to inform about incidents and security deficiencies without being fingered as “scapegoats”.

- In addition, monitor security problems in standard IT security components, as these are often the core or subcomponents of the IT solutions that control the ICS. A Cisco bug or a Windows bug can be just as serious as a security bug in the software that controls the ICS.

Participate in user associations, standardization bodies and other networks for security in ICS

Many international initiatives are currently underway to develop standards and recommendations for creating security in ICS. Many government entities in Europe, North America and Asia are highly prioritizing the area. By actively participating in this security work, users and vendors of ICS can influence which security requirements will be placed on these systems in the future.

By working through various national and international organizations and interest groups, it is possible for industrial information and control system users to set higher, clearer and more cohesive security requirements on vendors, system integrators and application developers.

By participating in security work it is possible for vendors of ICS, applications or other control equipment, to create a competitive advantage. Certain branches already have established security requirements. Power companies in the USA, for example, are expected to follow the NERC CIP standard. In the future, this will likely be a requirement in order to deliver both hardware and software.

Recommendations:

- Collaborate in user associations, social networks and organizations that develop expertise and support the members in their daily security work.
- Ensure that the representation is documented and that activities undertaken in each network are continuously reported to the employees concerned.
- Ensure management's familiarity with the representation and justify the way in which participation in the networks strengthens the security in the operations.

ABBREVIATIONS

ABWR	Advanced Boiling Water Reactors
ACE	Advanced Composition Explorer
ACG	Azeri-Chirag-Gunesli
AMI	Advanced Metering Infrastructure
ANL	Argonne National Lab
APWR	Advanced Pressurized Water Reactors
AQAM	Al-Qaeda and Associated Movements
BIS	Business Innovation and Skills
BP	British Petroleum
BPS	Bulk Power System
BTC	Baku-Tbilisi-Ceyhan
CAPEC	Common Attack Pattern Enumeration and Classification
CBRN	Chemical, Biological, Radiological and Nuclear
CCD COE NATO	Cooperative Cyber Defense Center of Excellence
CCE	Common Configuration Enumeration
CDA	Critical Digital Assets
CEI	Critical Energy Infrastructures
CEOS	Committee on Earth Observation Satellites
CEP	Civil Emergency Planning
CERT	Computer Emergency Response Team
CERT-UK	Computer Emergency Response Team United Kingdom
CI	Critical Infrastructure
C-I-A	Confidentiality, Integrity and Availability
CIEP	Clingendael International Energy Program
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CIKR	Critical Infrastructure Key Resource

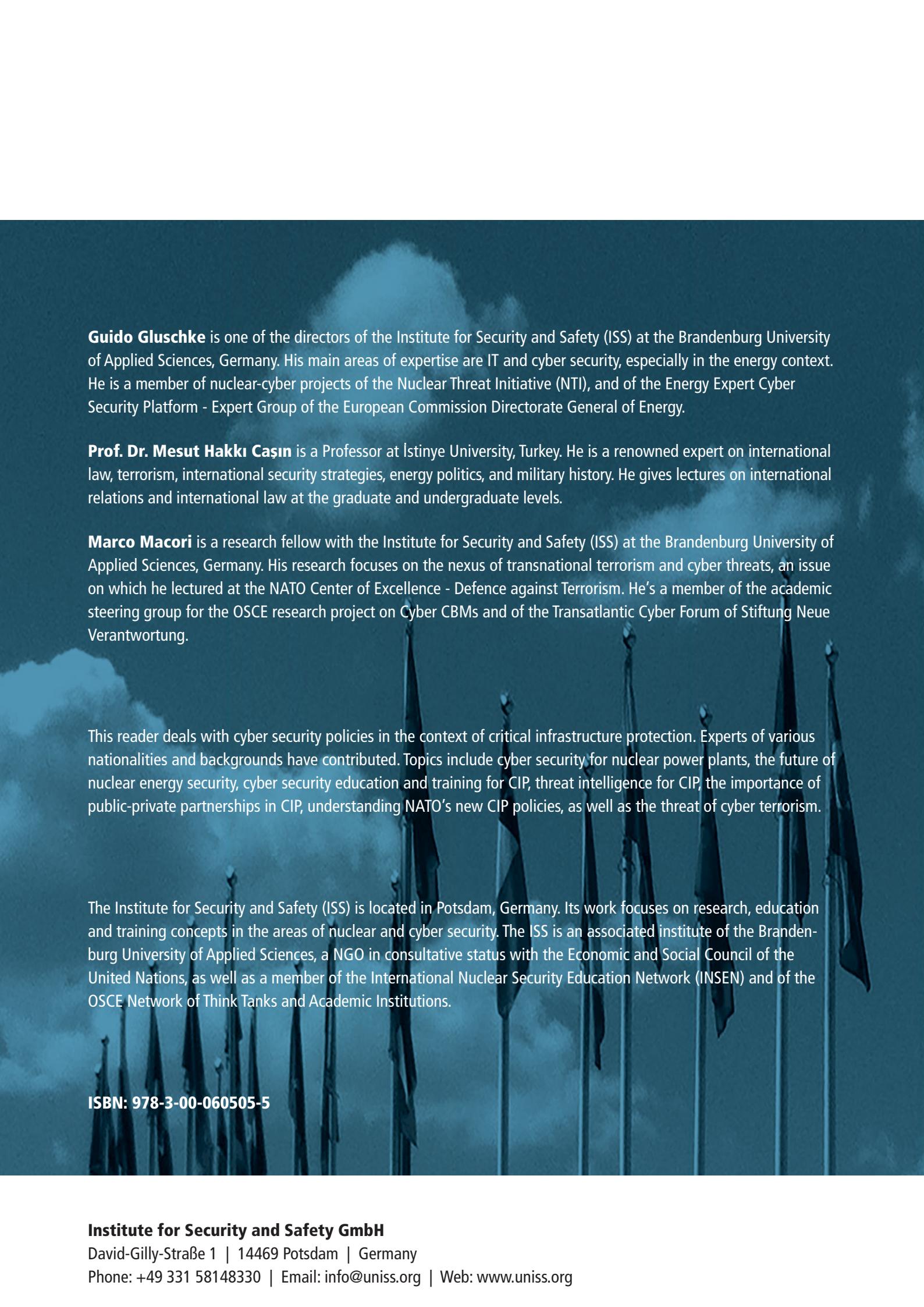
CIRT	Cyber Incident Response Teams
CPC	Caspian Pipeline Consortium
CPNI	Centre for the Protection of National Infrastructure
CRADA	Cooperative Research and Development Agreement
CRITS	Collaborative Research into Threats
CRPA	Cyber Security Risk Preparedness Assessment
CS&C	The Office of Cyber Security and Communications
CSI	Critical Space Infrastructures
CNSS	Committee on National Security Systems
CPE	Common Platform Enumeration
CR	Caspian Region
CS	Caspian Sea
CSA	Comprehensive Safeguards Agreement
CSMS	Cyber Security Management System
CSP	Cyber Security Plan
CRISP	Cyber Security Risk Information Sharing Program
CST	Cyber Security Team
CTBT	Comprehensive Nuclear-Test-Ban
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CybOX	Cyber Observable eXpression
DBT	Design Basis Threat
DCLG	Department for Communities and Local Government
DCS	Distributed Control Systems
DDos	Distributed Denial of Service Attacks
DeCM	Destructive Cyber Militancy
DHS	Department of Homeland Security
DMS	Demilitarized Zones
DoE	Department of Energy

DSO	Distribution Service Operators
EC-RRG	Electronic Communications Resilience and Response Group
E-ISAC	Electricity Information Sharing and Analysis Center
ENCS	European Network for Cyber Security
ENISA	European Network Information Security Agency
ENSREG	European Nuclear Regulators Group
ENCS	European Network for Cyber Security
ESCC	Electricity Subsector Coordinating Council
EU	European Union
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FI-ISAC	Financial Institutes–Information Sharing and Analysis Centre
FNS	Facility Network Security
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
GHG	Greenhouse Gas
GIS	Global Information Systems
GNSS	Global Navigation Satellite Systems
GridEx	Grid Security Exercise Series
GridSecCon	Grid Security Conference
GWe	Gigawatt-electric
HAN	Home Area Network
HLW	High Level Waste
HMI	Human Machine Interfaces
HSPD	Homeland Security Presidential Directive
IACS	Industrial Automation and Control Systems
IAEA	International Atomic Energy Agency
ICT	Information Communication Technologies
I&C	Instrumentation and Control Systems

ICS	Industrial Control System
IDS	Intrusion Detection Systems
IEA	International Energy Agency
IED	Intelligent Electronic Devices
IHD	In Home Display Unit
ILW	Intermediate Level Waste
ODEF	Incident Object Description Exchange Format
OpenIOC	Open Indicators of Compromise
IP	Office of Infrastructure Protection
ISAC	Information Sharing and Analysis Center
ISAOs	Information Sharing and Analysis Organizations
ISD	Information Sharing Device
ISHD	Islamic State Hacker Division
ISMS	Information Security Management System
I&C	Instrumentation and Control
IT	Information Technologies
KHNP	Korea Hydro and Nuclear Power
KINAC	Korea Institute of Nuclear Nonproliferation and Control
KWh	Kilowatt-hours
LEU	Low-Enriched Uranium
LLW	Low Level Waste
LNG	Liquefied Natural Gas
LWR	Light Water Reactors
MAEC	Malware Attribute Enumeration and Characterization
MJ	Mega Joule
MISP	Malware Information Sharing Platform
MN CD2	Multinational Cyber Defense Capacity Development
MN CD E&T	Multinational Cyber Defense Education and Training
MoU	Memorandum of Understanding

MSIP	Ministry of Science, Information and Communication Technology and Future Planning
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Center
NCIRC	NATO Computer Incident Response Capability
NDPP	NATO Defense Planning Process
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIS	National Intelligence Service
NIST	National Institute for Standards and Technology
NNWS	Non-Nuclear Weapon States
NOAA	National Oceanic and Atmospheric Administration
NPP	Nuclear Power Plant
NPT	Nuclear Non-Proliferation Treaty
NRC	National Research Council
NSIS	National Strategy on Information Sharing
NSSC	Nuclear Safety and Security Commission
NSS	Nuclear Security Summit
NSS	Nuclear Security Summit
OECD	Organization for Economic Co-operation and Development
OSCE	Organization for Security and Cooperation in Europe
OVAL	Open Vulnerability and Assessment Language
PBX	Private Branch Exchange
PCCIP	President's Commission on Critical Infrastructure Protection
PII	Personal Identifiable Information
PLC	Programmable Logic Controller
PNNL	Pacific Northwest National Labs
PP	Pipeline Protection
PPD	Presidential Policy Directive

PPP	Public-Private Partnership
PWR	Pressurized Water Reactor
UK	United Kingdom
UNCLOS	UN Convention on Law of the Sea
US	United States
UTM	Unified Threat Management
TAEA	Turkish Atomic Energy Agency
TAXII	Trusted Automated eXchange of Indicator Information
TI-EPF	Telecoms Industry Emergency Planning Forum
TLP	Traffic Light Protocol
TTP	Tactic, Technic, Procedure
TWh	Terawatt-hours
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SSEP	Safety, Security, Emergency, Preparedness
SETA	Security Education, Training and Awareness
SPPD	Strategic Pipeline Protection Department
STIX	Structured Threat Information eXpression
UN	United Nations
UNSC	UN Security Council
US	United States
WAN	Wide Area Network
WTC	World Trade Center
XCCDF	eXtensible Configuration Checklist Description Format
3S	Security, Safety and Safeguards



Guido Gluschke is one of the directors of the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, Germany. His main areas of expertise are IT and cyber security, especially in the energy context. He is a member of nuclear-cyber projects of the Nuclear Threat Initiative (NTI), and of the Energy Expert Cyber Security Platform - Expert Group of the European Commission Directorate General of Energy.

Prof. Dr. Mesut Hakkı Caşın is a Professor at İstinye University, Turkey. He is a renowned expert on international law, terrorism, international security strategies, energy politics, and military history. He gives lectures on international relations and international law at the graduate and undergraduate levels.

Marco Macori is a research fellow with the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, Germany. His research focuses on the nexus of transnational terrorism and cyber threats, an issue on which he lectured at the NATO Center of Excellence - Defence against Terrorism. He's a member of the academic steering group for the OSCE research project on Cyber CBMs and of the Transatlantic Cyber Forum of Stiftung Neue Verantwortung.

This reader deals with cyber security policies in the context of critical infrastructure protection. Experts of various nationalities and backgrounds have contributed. Topics include cyber security for nuclear power plants, the future of nuclear energy security, cyber security education and training for CIP, threat intelligence for CIP, the importance of public-private partnerships in CIP, understanding NATO's new CIP policies, as well as the threat of cyber terrorism.

The Institute for Security and Safety (ISS) is located in Potsdam, Germany. Its work focuses on research, education and training concepts in the areas of nuclear and cyber security. The ISS is an associated institute of the Brandenburg University of Applied Sciences, a NGO in consultative status with the Economic and Social Council of the United Nations, as well as a member of the International Nuclear Security Education Network (INSEN) and of the OSCE Network of Think Tanks and Academic Institutions.

ISBN: 978-3-00-060505-5