Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Confidence-Building Measures in Cyber

M.Sc. Kristina Sander
Institute for Security
and Safety GmbH (ISS)
at Brandenburg University
of Applied Sciences

David-Gilly-Str. 1
14469 Potsdam
Germany

Phone +49-331-58148330
Web www.uniss.org
E-Mail info@uniss.org

Potsdam, July 7, 2018

Content

List of tables

List of abbreviations

ASEAN	Association of Southeast Asian Nations
ARF	ASEAN Regional Forum
CBM	Confidence-building measure
ICT	Information and Communication Technology
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OSCE	Organization for Security and Co-operation in Europe
OSCE PC	Permanent Council of the Organization for Security and Co-operation in Europe
UN	United Nations
UN GGE	United Nations Group of Governmental Experts

1 Introduction

In times of the information age zero-day vulnerability exploits have gained a main role in information warfare. Experts state the next great conflict will not be taking place on physical terrain but in the electric spectrum.[1] The cyber-attacks in Estonia in 2007, following the take down of a historic soviet war monument, is just one example where a wave of denial of service attacks highlighted the vulnerabilities in cyberspace that allow an adversary to cause a mess on governments from hundreds or thousands miles away. The attacks emphasize the urgency for more comprehensive measures that reinforce existing cybersecurity.[2]
As protection of cyberspace and reducing its vulnerabilities to digital threats has become a key element of national security strategies state and non-state actors still increase their exploitation of vulnerabilities in cyberspace to gain advantage over their competitors and adversaries. Thus, the competition for the 'digital supremacy' is increasing the risk of escalation and conflict. As ICT is being turned into weapons, an increasing number of states give some role to the armed forces: 12 out of 12 largest military spenders are developing dedicated cyber warfare units and two-thirds appear to possess or be developing offensive cyber capabilities.[3] E.g. the US Army, already owning 30 cyber teams, was aiming to have 41 fully operational teams by the end of 2017 that demonstrates cyber weapons are a key interest of the new US administration.[4] Not only the US but many other countries have also been investing in offensive and defensive cyber capabilities of military nature. Considering the reliance on information and communication technology (ICT) for the delivery of governmental, financial and public services, states and the public society are at severe risk for cyber-attacks.[5]
In view of the imbalance that could cause an international conflict and instability, first measures and actions have been initiated by international communities to build confidence between states.
Therefore this paper aims, to elaborate the evolution of confidence- building

[1] Tucker (2017), pp.2-3
[2] OSCE (2016), pp.5-6
[3] NATO CCD COE (2016), pp.129-131
[4] Tucker (2017), p.3
[5] NATO CCD COE (2016), pp.129-131

measures (CBMs) in cyber after outlining the evolution of traditional CBMs in the last century.

2 Traditional Confidence-Building Measures

CBMs are a key mechanism aiming to prevent or to reduce the risk of a conflict by eliminating the causes of mistrust, misunderstanding and miscalculation between states. Their primary focus is to increase transparency, improve information exchange, and to restrain the use of violence by armed forces. They are a tool to ensure that nation states have the same understanding of the normative commitments they agreed on.

CBMs can be understood as a series of actions that are negotiated, agreed and implemented by the parties in order to build confidence, without specifically focusing the root causes of the conflict. Only when the purpose behind a given action is to increase confidence between parties and no other motives, the measures are considered as CBMs.[6] 'CBMs by themselves will not solve a conflict but they can modify relations and behavior and thereby the context which the conflict resolution process takes place. It should be understood as an investment in the broader objective of peace rather than as objective themselves.'[7] Thus, the aim is not to address the root cause of a conflict.[8] They are of limited use when conflicts are fueled intentionally.[9]

CBMs have been used for centuries but only in the second half of the last century they were looked at in a more systematic way. They were evolved during the early days of the Cold War to increase transparency between two military adversaries. The need for effective communication channels became obvious after the Cuba Crisis to prevent a nuclear attack on either side caused by a misunderstanding. The Helsinki Act was the first generation of agreed CBMs that further evolved in the Stockholm Document in 1986 which was the first security agreement for Europe with political and military binding CBMs. In 1990 they were expanded in the Vienna Document by a series of measures covering immediate risk reduction and long-term routine military interaction. During the Cold War the focus was especially on military CBMs rather than on non-military CBMs.

[6] Mason, S. and Siegfried, M. (2013), pp.58-59
[7] OSCE (2012), p.11
[8] Mason, S. and Siegfried, M. (2013), pp.57-59
[9] NATO CCD COE (2016), p.135

Military CBMs aim to prevent a potential outbreak of military conflict by improving relations between governments and militaries. [10] They primarily used to reduce military tensions and the fear of a surprise attack. They usually consist of measures like military data exchange or pre-notification of military movements or exercises.[11]
Non-military measures concentrate on preserving peace by building trust between communities and include actions across the political, economic, environmental, social and cultural field:[12]

- Political: e.g. power sharing, electoral reform and decentralization of power, democratization measures
- Economic: e.g. economic co-operation and thereby remove barriers of mistrust; Actors seldom risk their economic well-being.
- Environmental: collaborative planning and training in joint response to natural and man-made disasters
- Societal: networks of people-to-people activities, dialogues and joint projects that create the foundations; e.g. dialogue between educators and journalists, academic conferences, workshop and joint research projects, etc.
- Cultural: demonstrate a governments sensitivity to local cultures and show respect for traditional authorities; e.g. avoiding the declaration of a single official language when the state includes a significant ethnic minority group which uses another language or demonstrating respect for cultural leaders and local practices like exercising sensitivity on issues such as removing monuments meaningful to certain ethnic groups.[13]

The OSCE allocates CBMs certain characteristics, inter alia:

- Reciprocity: measures should lead to similar measures being taken by each party in a balanced and reciprocal manner.
- Incremental: CBMs are implemented progressively in evolutionary stages of increasing significance.
- Long-term: Confidence is a process which needs time. CBMs hardly ever yield results in the short term.

[10] NATO CCD COE (2016), p.132
[11] OSCE (2012), pp.11-14
[12] NATO CCD COE (2016), p.132
[13] OSCE (2012), pp.9-10

- Predictability: Both sides should act predictably and the CBM framework should promote predictable behavior.
- Transparency: The intention should be obvious, open and unambiguous.
- Reliability: A CBM as a tactical maneuver is likely to complicate relations even further. Not carrying through a CBM that is already initiated is likely to have a similar effect.
- Consistency: CBMs should be consistent with regard to their topics or the message they send. Inconsistency will lower their impact or lead an entire CBM process to failure.
- Communication: CBMs need appropriate communication channels between parties to facilitate information flow in order to address misunderstandings.
- Verification: CBMs where reciprocity is expected, verification and monitoring are an important component in allying fears and mistrust.
- Local ownership: CBMs rarely succeed when they are imposed on the parties from outside. They depend on the voluntary engagement of both sides.
- Multi-Level: CBM process is built on both elements, involving government structures and civil society. CBMs can be bottom-up or top-down.[14]

Involved in the process and negotiating of CBMs are usually three different types of actors: negotiators, decision-makers and the wider constituencies.
While negotiators trust each other and are working towards an agreement the decision-makers is the elite and political, security, economic and social decision-makers. They usually do not negotiate at the table. Wider constituencies are affected by the negotiations as they need to develop the confidence. Many initiatives bring together representatives from wider constituencies that can create an atmosphere of trust. CBMs can therefore also be developed by these representatives.[15]

[14] OSCE (2012) pp.16-18
[15] Mason, S. and Siegfried, M. (2013), p.62

3 The nature of cyberwarfare and cyber-attacks

Among international policymakers the debate of defining a certain level of a cyber-attack as an armed attack has still not reached consensus. There is no general idea today what is meant by the 'armed attack' in relation to the use of ICTs.[16] The definitions of cyber weapons and cyberwarfare are not much more precise than in 2010 when the Stuxnet attack shut down one of Iran's nuclear enrichment facilities. Although the Pentagon confirmed a secret list of cyber weapons in 2011, using it as deterrence or not, details about the weapons were kept unknown.[17] The nuclear warfare gave an understanding of deterrence that is dissimilar to cyberwarfare. Attacks, be they be conventional or nuclear, were always assumed to be attributable. The heart of cyberwarfare though is the problem of attribution.[18] The cyberspace enables certain levels of anonymity that state, state-sponsored and non-state actors do not shy from exploiting. The difficulties attributing an attack give actors the ability to deny responsibility. The uncertainty regarding attribution and the absence of a common understanding regarding acceptable behavior may create instability and misperception.[19] The unique feature and at the same time the biggest concern of digital weapons is the lack of information about the adversary's capabilities. Looking back at the Cold War, adversaries had a rough idea of each other's divisions, ships or planes. But cyber weapons are opaque. It is hard to reach a degree of certainty.[20] Consequently, from the current knowledge this reduces confidence-building in cyber on non-military rather than military measures.

[16] NATO CCD COE (2016), p.133
[17] Tucker (2017),p.3
[18] Gelinas (2010), p.1-4
[19] NATO CCD COE (2016), p.130-133
[20] Tucker (2017), p.5

4 Confidence Building Measures in Cyber

The international community has engaged in several processes focused on clarifying how the existing international law applies to cyberspace, how to develop norms of responsible state behavior and how to evolve confidence-building measures in cyber. There have been efforts by four multiple consecutive international and regional groups of governmental experts on.[21] Table 1 gives a chronical overview of steps and milestones towards CBMs in cyber.

Table 1: Chronical overview of steps and milestones towards the development of CBMs in cyber.

Year	Organization	Development
1998	UN	Introduction of the issue of information security in the international context by Russia
2002	OAS	At the meeting of the Committee on Hemispheric Security the Permanent Council addressed the security of critical information systems and considered the need to develop a cyber security strategy.
2003	UN Report of the Secretary-General to the General Assembly	Russia putting forward the idea of establishing an international group of governmental experts to analyze international legal provisions relating to various aspects of international information security and study existing concepts and approaches.
2004	UN GGE	The international group of governmental experts, initiated by Russia's idea in 2003, did not reach consensus on the final report due to the complexity of the issue.
2004	OAS	Adoption of a comprehensive inter-American cybersecurity strategy that encompasses a number of initi-

[21] NATO CCD COE (2016), p.129-131

		atives aimed at strengthening trust and confidence in cyberspace.
2010	UN GGE report	The report emphasizes the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to state use of ICTs and calls for measures to build confidence, reduce risk and enhance transparency and stability.
2012	OSCE PC Decision No. 1039	Decision on establishing an open-ended and informal OSCE working group tasked with the elaboration of a set of draft CBMs.
2013	OSCE Istanbul Declaration	The Declaration urges the OSCE to develop CBMs.
2013	UN GGE report	The report emphasizes that voluntary CBMs can promote trust and assurance among states and help reduce the risk of conflict by increasing predictability and reducing misperception.
2013 (Dec.)	OSCE PC Decision No. 1106	OSCE launched a process to adopt a set of eleven voluntary CBMs in cyberspace.
2014	ARF Ministerial Meeting	ARF is mandated to develop a work plan on ICT security focusing on a practical cooperation on CBMs. Therefore the ARF organized a series of seminars on CBMs in cyberspace and other events focusing on broader issues, including cyber incident response.
2015	UN GGE report	The report recommends that sates cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may expose threats to international peace and stability. The report therefore proposes a catalogue of CBMs that supplements consensus of the OSCE.
2015	ARF Ministerial Meeting	A work plan is presented to promote a peaceful, secure, open and cooperative ICT environment and to prevent conflicts and crisis by developing trust and confidence between states in the ARF region. The objectives include promoting transparency and de-

		veloping confidence-building measures to enhance the understanding of ARF countries in the ICT environment. The Plan proposes a Study Group on CBMs.
2016	OSCE PC Decision No. 1202	In Decision No. 1202 the OSCE adopts further CBMs to the set, developed in 2013.

The issue of information security in the international context was introduced to the United Nations agenda by Russia in 1998. Since then, the Secretary-General to the General Assembly has presented annual reports laying out the views of Member States. In its submission to the 2003 report, Russia put forward the idea of establishing an international group of governmental experts which would analyze international legal provisions relating to various aspects of international information security and study existing concepts and approaches. A UN group of global governmental experts phrased reports that evolved the urge and need for confidence-building in cyber but never reached a set of agreed CBMs. The biggest breakthrough was the UN GGE report in 2015 proposing a catalogue of CBMs that aligned with the set evolved by the OSCE.[22]

Another initiative, the ASEAN (Association of Southeast Asian Nations) Regional Forum (ARF), one of the main forums for the discussion of CBMs in Asia presented, agreed on confidence-building, preventive diplomacy and conflict resolution in 1995. In 2014 at the ARF Ministerial Meeting the ARF was mandated to develop a work plan on security for ICT focusing on practical cooperation on CBMs. The ARF organized a series of seminars on CBMs in cyberspace and other events focusing on broader issues. The work plan was presented at the Ministerial Meeting in 2015 aiming to promote a peaceful, secure, open and cooperative ICT environment and to prevent conflict and crises by developing trust and confidence between states in the ARF region, and by capacity building. The work plan proposed to establish open-ended study groups on CBMs.

Yet another initiative, the Organization of American States (OAS), took a different approach by directly defining cooperative measures. Holding conferences resulting in the development of two comprehensive sets of CBMs, the meeting of the Committee on Hemispheric Security of the Permanent Council in 2002 first addressed the security of critical information systems and considered the

[22] NATO CCD COE (2016), p.136

need to develop a cyber security strategy. In 2004 a Comprehensive Inter-American cyber-security strategy followed that included a number of initiatives aiming to strengthen trust and confidence in cyberspace. E.g. it held the idea of building an inter-American alert, watch and warning network to rapidly disseminate cyber security information and respond to crises and incidents or identifying and adopting technical standards for a secure Internet architecture. Since the adoption of the strategy, cooperation between responsible national authorities such as CERTS and law enforcement agencies has improved consistently with regard to information sharing and technical cooperation. Still some of them suffer to meet the basic needs for advancing their technical and investigative capabilities and requisite laws in place, while others do not, which did not dissolve an imbalance.[23]

While many international organizations, groups or initiatives followed up on the security issues in cyberspace the only project to develop a set of agreed was the OSCE.

In 2012 the OSCE PC decided to establish an open-ended and informal OSCE working group tasked with elaboration of a set of draft confidence-building measures. [24] The working group was tasked to 'elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs', to ' build consensus for the adoption of such a set of CBMs in 2012' and to ' provide progress reports, in consultation with members of the working group, who will report to the PC'.[25]

A decision on CBMs as a proposal for a Ministerial Council was discussed at the 2012 Ministerial Council 2012 in Dublin but did not reach consensus due to objections by Russia.[26] In result of that the Istanbul Declaration of 2013 urged the OSCE to develop CBMs and the OSCE launched a process to adopt a set of CBMs. A historical compromise on a set of eleven voluntary CBMs in cyberspace was found and published in Decision 1106 in Dec 2013. It held a plan for implementation by the adoption of transparency measures, the development of cooperative measures and the adoption of stability measures.[27] The set of the eleven CBMs can be distinguished by their type (see also Appendix p.17):

- Transparency measures: CBM No. 1,4,7, 9, 10
- Cooperative measures of non-military nature: CBM No. 2, 3, 5, 6,8, 11[28]

[23] NATO CCD COE (2016), pp.144-146
[24] NATO CCD COE (2016), p.137
[25] OSCE Permanent Council (2012), p.1
[26] NATO CCD COE (2016), p.137
[27] NATO CCD COE (2016), pp.137-140
[28] OSCE Permanent Council (2013), pp.1-4

Following the initial set of CBMs from 2013, the OSCE working group agreed on five additional measures in Decision No. 1202 in 2016 extending the first set (see also Appendix p.20).

Three measures were added to the set of the elven ore measures. One additional measures, CBM No. 16 for encouraging 'responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities' can also be assigned to the type 'transparency'. Further measures of Decision No. 1202 can be assigned to the type 'cooperative measures of non-military nature': CBM No. 12 for facilitating 'inter-state exchange in different formats including workshops, seminars, and roundtables, including on the regional and/or sub regional level'. The objective of those activities is to prevent conflicts stemming from the use of ICTs and to maintain the peaceful use of ICTs. Another measure that can be assigned to the type 'cooperative measures of non-military nature' is CBM No. 13 for conducting 'activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict' and CBM No.15 for encouraging and facilitating in 'regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies', e.g. sharing information on ICT threats or exchanging best practices.

CBM No. 14 could be assigned to one type as it aims to 'promote public-private partnerships consistent with national legislation and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs' within a state and not between states.[29]

[29] Organization for Security and Co-operation in Europe (OSCE) Permanent Council (2016), pp.1-13

5 Discussion

Comparing the CBMs developed for cyber one cannot miss out that not all dimensions of the traditional CBMs were able to be transferred. Agreements on transparency measures and on cooperatives measures of non-military nature could be found. [30] Looking closer at the intention of CBM No.8 it could almost be stated that its intention can be compared to the idea of an environmental measure by adopting co-operations in case of cyber incidents. The author of NATO CCD COE's paper assigns CBM No.3 - consultations to reduce the risk of misperception, military conflict or tension- and CBM No.4 -sharing information on taken measures-, CBM No. 7 -sharing information on national organization, strategies and policies- and CBM No. 9 -providing a list of national terminology- to measures of transparency and verification. But looking back at the original idea in sense of traditional CBMs it rather intended the monitoring of military facilities and activities, e.g. by inviting observers to monitor major military exercises. Exchanging information about strategies and measures may not fulfill the original intention of transparency and verification, if anything then transparency. It is one difficulty of confidence-building in cyber given the dual-nature of cyber-tools and countries' interest in preserving strategic ambiguity concerning their capabilities. As mentioned before, no military restraint measures were developed or agreed on. Considering the civil-military nature of the Internet and the lack of transparency, what is considered a cyber-weapon and who would count as a nation state actor, it is difficult to define CBMs. It would require a weapon-free zone in cyberspace in terms of ICT infrastructure. Furthermore attacks are hard to be linked to geographic boundaries. Yet two other traditional CBMs that have not been met yet are societal and cultural measures and economic measures. Considering CBM No. 9 -providing a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term-, an international agreement not only on terminology but further on the definition of an attack and its attribution, seems to represent a major challenge ahead. There needs to be a clear definition of cyber military

[30] NATO CCD COE (2016), pp.142-143

capabilities and a clear separation of military and civilian capabilities to take full advantage of measures aiming for transparency.

The suggested CBMs for cyber assume that states have a certain level of capabilities that gives them the possibility to implement them. To foster the implementation of CBMs one major trend should be focused on building states' cyber capacities to ensure that all countries meet certain baseline levels that enable them to participate. Another major trend should be to spread the implementation of CBMs as bilateral transparent cyber pacts between states that are more politically binding.[31] Examples of recent years are the US-Russia agreement in 2013, the Russia-China agreement from 2015 or the US-China agreement from 2015. But since the public knowledge about the content of the agreements is limited, it is hard to assess their effectiveness.[32]

At the current state new boundaries of cyber warfare are still being explored and discovered and are not expected to be exhausted yet.[33] Where there is no political will for negotiations, CBMs alone are unlikely to make the difference.[34] And even if 'confidence can be built through dialogue alone, there is always the danger of misunderstandings and the possibility of intentionally misleading each other with words. Actions can also be misinterpreted in a hostile environment, yet because actions require greater effort than words, they are generally more credible and useful in helping conflict parties read each other's intentions'.[35] Hence, although there might be a limited political will, CBMs turn out to be the best option to gain political stability in cyber as even international treaties only provides an illusion of it.[36]

[31] NATO CCD COE (2016), p.146
[32] NATO CCD COE (2016), pp.146-149
[33] Tucker (2017), pp.2-5
[34] Mason, S. and Siegfried, M. (2013), P.57
[35] Mason, S. and Siegfried, M. (2013), p.59
[36] NATO CCD COE (2016), p.133

6 Conclusion

Multiple international working groups and initiatives have recognized the need for the development of CBMs for cyber. Today, the cyberspace and its vulnerabilities are still being exploited for on sides' supremacy or advantage. Consensus has not been reached on setting the lines. The set of non-military CBMs developed by the OSCE has pushed their evolution further ahead. A next step, which has already been initiated by the OSCE, would be to assess and evaluate the implementation of CBMs. In an interview with an official of OSCE it was emphasized that the implementation of the CBM process is becoming more mature. E.g. Nation states reached consensus in providing crisis communication channels in order to prevent escalation in case of cyber conflicts. But looking back at the origin of CBMs during the Cold War, that were developed and improved for more than over 50 years, there still might be a long way to go. Keeping that in mind CBMs in cyber could just be in their infancy.

7 References

Gelinas, R. R. (2010). Cyberdeterrence and the Problem of Attribution. Georgetown University, Washington, DC. Retrieved from https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/historical/gelinasRyan.pdf

Mason, S. and Siegfried, M. (2013). Confidence Building Measures (CBMs) in Peace Processes. *Managing Peace Processes: Process related questions. A handbook for AU practitioners*, *2013*(1), 57–77.

NATO CCD COE (Ed.). (2016). *International Cyber Norms: Legal, Policy & Industry Perspectives*. Talinn, Estonia. Retrieved from https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html

Organization for Security and Co-operation in Europe (OSCE). (2012). OSCE Guide on Non-military Confidence-Building Measures (CBMs). Retrieved from https://www.osce.org/secretariat/91082?download=true

Organization for Security and Co-operation in Europe (OSCE). (2016). Update Paper. Retrieved from https://www.mensenhandelweb.nl/sites/default/files/NHSMUN%202016%20OSCE%20Update%20Paper.pdf

Organization for Security and Co-operation in Europe (OSCE) Permanent Council. (2012). Decision No 1039 Development of Confidence-Buidling Measures to Reduce the Risks of Conlict Stemming from the Use of Information and Communication Technologies. Retrieved from file:///H:/Master%20Security%20Management/Cyber%20War/Auswahl/pcdec1039_reduce_risk_of_conflicts_from_use_of_ICT.pdf

Organization for Security and Co-operation in Europe (OSCE) Permanent Council. (2013). Decision No 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Retrieved from https://www.osce.org/pc/109168?download=true

Organization for Security and Co-operation in Europe (OSCE) Permanent Council. (2016). 1092nd Plenary Meeting of the Council. Retrieved from https://www.osce.org/pc/227791

Tucker, P. (2017). *Cyber Warfare: April 2017 Ebook*. *Defense One*.

Appendix

OSCE Decision No. 1106

The OSCE participating States in Permanent Council released in December 2013 a set of agreed CBMs to reduce risks of conflict stemming from the use of information and communication technologies (ICTs). The set held 11 CBMs that can be distinguished by their type:

- Transparency measures:
    - 1: Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.
    - 4: Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.
    - 7: Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.
    - 9: In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.
    - 10: Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

- Cooperative measures of non-military nature:
    - 2: Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.
    - 3: Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.
    - 5: The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.
    - 6: Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.[37]
    - 8: Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and coordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.
    - 11: Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates

[37] OSCE Permanent Council (2013), pp.1-2

for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

OSCE Decision No. 1202

The following CBMs were added to the initial set of 2013 by the OSCE working group:

- 12: Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or sub regional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs. Inter alia:
    - Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability
    - Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and
    - Take into account the needs and requirements of participating States taking part in such activities.
    - Participating States are encouraged to invite and engage representatives of the private sector, academia, centers of excellence and civil society in such activities.
- 13: Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No.1106.
- 14: Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.
- 15: Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and sub regional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

  Inter alia:
    - Sharing Information on ICT threats

- Exchanging best practices;
- Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure
- Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident
- Sharing national views of categories of ICT-enabled infrastructure States consider critical
- Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and sub regional levels; and
- Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

- 16: Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No.1106, with a view to avoiding duplication.[38]

[38] OSCE Permanent Council (2016), pp.1-13