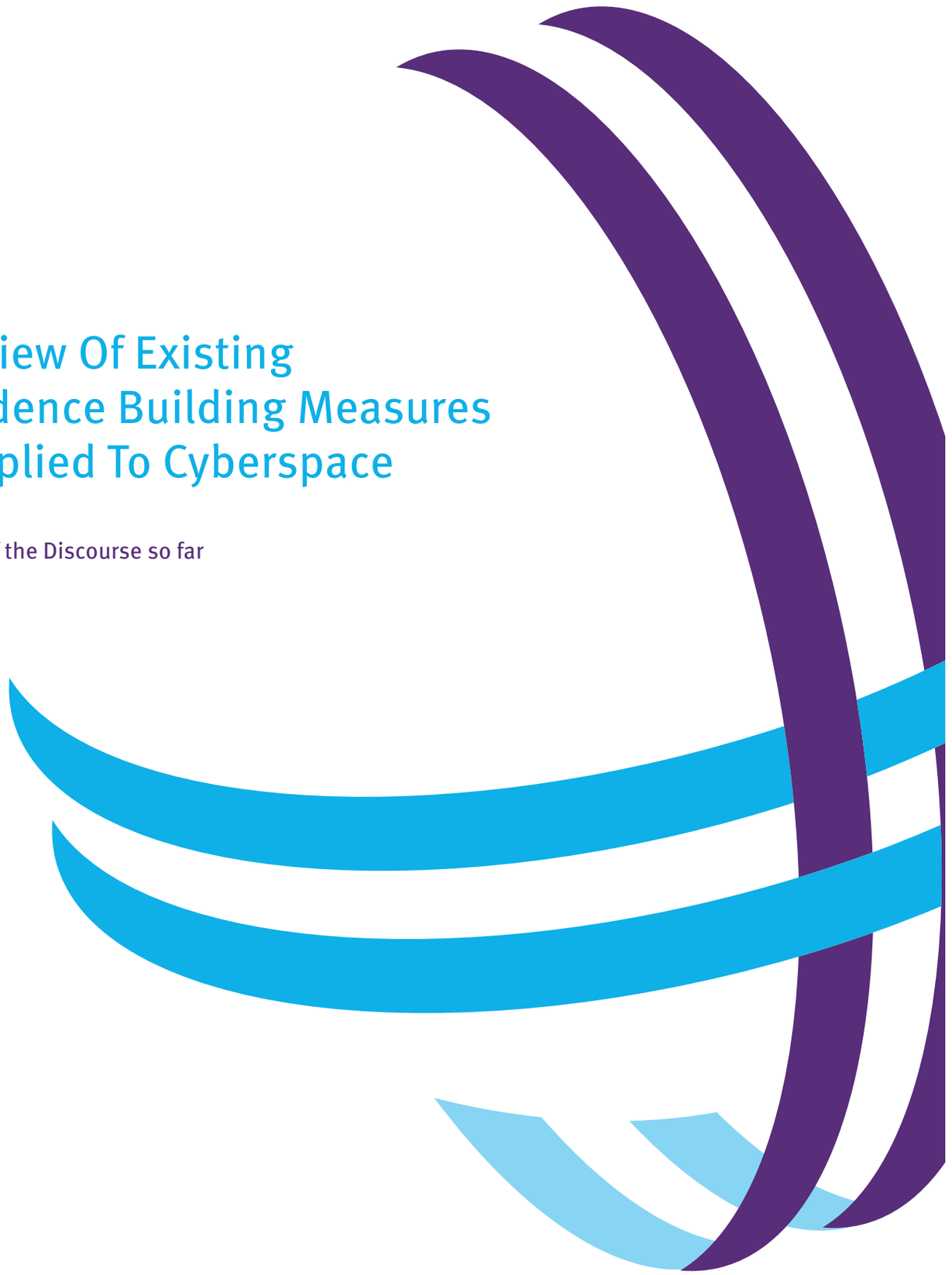


Overview Of Existing Confidence Building Measures As Applied To Cyberspace

Overview of the Discourse so far

Authors

This paper was developed as part of the workplan of the Global Forum for Cyber Expertise's (GFCE) Task Force on CBM and Norms Implementation & Cyber Diplomacy, under the direction of the Task Force Leads Kaja Ciglic and Nikolas Ott. They wish to thank for their contributions or comments the Centre for Internet and Society, Microsoft, New America, Organization of American States (OAS), and Organization for Security and Co-operation in Europe (OSCE).

Publication Date - 03/06/2020

Table of Contents

About the GFCE

Everyone should be able to fully reap the benefits of Information and Communicate Technology (ICT) through a free, open, and secure digital world.

The Global Forum on Cyber Expertise (GFCE) was launched at the Global Conference on Cyber Space in The Hague based on this vision.

The GFCE was tasked with a clear mission to strengthen cyber capacity and expertise globally by being a pragmatic, action-oriented and flexible platform for international co-operation.

The unique structure of the GFCE as a bottom-up, neutral and apolitical forum provides an excellent opportunity for multi-stakeholders to exchange best practices and expertise on cyber capacity building.

GFCE Working Groups

Members and partners work together on cyber capacity building through Working Groups. The GFCE Working Groups are based on the five prioritized themes in the Delhi Communiqué[1], seeking to encourage multistakeholder dialogue on the implementation of cyber capacity building: bringing together needs, resources and expertise. **The five themes are:**

- Cybersecurity policy & strategy;
- Cyber incident management & critical information protection;
- Cybercrime;
- Cybersecurity culture & skills;
- Cybersecurity standards.

Working Group on Cybersecurity policy and strategy

The theme of cybersecurity policy and strategy can be seen as the foundation of the other identified themes in the Delhi Communiqué. The aim of the group is thus to help countries and other stakeholders improve their policy and strategy making capacity. Recognizing the importance of the international cyber Confidence-Building Measures (CBMs) and Norms efforts, the Working Group formed a new Task Force on CBMs and Norms Implementation & Cyber Diplomacy at the Internet Governance Forum (IGF) in 2018.

The Task Force focuses on practical cyber capacity building with regards to CBMs, norms implementation and cyber diplomacy and aims to empower countries to be able to engage on these topics. In 2019, the Task Force mapped existing CBMs and norms, and identified key stakeholders, actors, and events in this space. The Task Force has also mapped over 50 cyber capacity building projects and developed a repository of relevant tools and publications on Cybil[2], the CCB Knowledge Portal. At this stage, the Task Force seeks to bridge countries with the complex international cyber discussions and explore ways to support the practical implementation of the outcomes of such discussions.

For more information on the Task Force, please contact the GFCE Secretariat at contact@thegfce.org.

1 Delhi Communique: https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique
2 https://cybilportal.org/

What are confidence building measures?

Confidence Building Measures (CBMs) are not a new tool in the international diplomacy toolbox. Over the past century they have helped to defuse tensions on numerous occasions, as well as served to guide states' behavior resulting in more stable and predictable international relations.

CBMs are typically defined as actions and processes designed to reduce or eliminate the causes of mistrust, tensions and hostilities between and among states that could fuel arms races or lead to escalations and actual conflicts.

In many ways, they have traditionally acted as pressure valves. This has been done through enhancing states' understanding of one another's government structures, threat perceptions, and military capabilities. For example, within the military realm, advance notice of military maneuvers and exercises, and greater transparency in military budgets, strategic doctrine, and legal interpretations all serve as valuable CBMs that can reduce suspicions about, and increase understanding of other nations' capabilities and intent. Probably the most well-known example of a CBM is the establishment of a "hot line", a direct line of communication, between two heads of state that can help to quickly clarify any misperceptions that could have significant consequences.

Given their demonstrable effectiveness in ameliorating risk of military conflict, the use of CBMs has expanded to touch on the economic, environmental, and societal sectors as well. This includes the development of joint infrastructure and community development projects, joint responses to disaster relief, and the establishment of working groups to facilitate person-to-person exchanges to promote tolerance and mutual understanding. In each instance, these CBMs are tailored to the specific context governments are trying to address, but the underlying ambition remains the same: build trust and increase confidence among parties to a potential conflict.

Furthermore, the use of CBMs may, over time, result in other beneficial outcomes as well. They can help identify and address potential areas of disagreement in terms of the background norms (or laws) for state behavior. In addition, in areas where there is limited agreement on what international legal principles might apply, CBMs can serve as bridges to a common understanding of what acceptable international norms of behavior might be. As such, CBMs can act as precursors to the establishment and reinforcement of international norms.

Characteristics identified by the Organization for Security and Co-operation in Europe (OSCE) for successful non-military CBMs	
Reciprocity	Although short-term situations may be unequal, the long-term measures, concessions, commitments and advantage must be balanced and mutually acceptable.
Incremental	Starting with merely symbolic measures, CBMs may be progressively implemented in evolutionary stages of increasing significance.
Long-term	Irrespective of any short-term progress or temporary set-backs, CBMs need to achieve sustained results on the long run.
Predictability	As unpredictable behaviour may trigger unintended responses, the nature, scope and content of CBMs should promote parties' predictable behaviour.
Transparency	The intent and modalities of a CBM should be obvious, open and unambiguous. There should be no room for misinterpretation of its purposes.
Reliability	Proposed CBMs need to be realistic, and already initiated CBMs need to be carried through. Hence, CBMs need to be reliable.
Consistency	CBMs should be consistent with regard to topics, messages or target groups. Inconsistency will eventually lead to mistrust that undermines the entire CBM process.
Communication	Appropriate communication channels are required to provide for direct dialogue to clarify potential misunderstandings, misperceptions or mistakes.
Verification	Particularly in cases where reciprocity is expected, verification (possibly by third parties) is an important component in reducing parties' fear and mistrust.
Local ownership	The successful long-term implementation of CBMs depends on the voluntary engagement and real commitment of all parties. To that extent the interests, concerns, needs and priorities of all relevant parties must be taken into account.
Multi-level	CBMs can be developed top-down or bottom-up, but involvement of both government structures and civil society at large is an essential prerequisite for lasting success.

3 https://www.osce.org/secretariat/91082?download=true

Overview of efforts to establish confidence building measures for cyberspace

Efforts to design effective CBMs for cyberspace have been undertaken at both multilateral and bilateral levels. However, the development and implementation of cybersecurity CBMs is relatively recent. More work will need to be done to encourage their wider implementation. Despite that they have already contributed to advancing the dialogue on cyber stability. In addition, the discussions around CBMs adoption have resulted in the creation of important platforms that enable governments to have a conversation around these important issues.

It is worth highlighting that enabling these conversations can, by facilitating an exchange on the subject between governments, also be considered a confidence-building measure in its own right.

UN Group of Governmental Experts

At the multilateral level, cyber stability has been firmly on the agenda of the United Nations (UN) and its Groups of Governmental Experts (GGEs) since the early 2000s. In their 2010 report [4], the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security recommended five actions for the development of confidence-building and other measures to reduce the risk of misperception resulting from cyber disruptions. These actions included:

- elaborating common terms and definitions necessary to advance dialogue in the information security field;
- identifying measures to support capacity building in less developed countries; as well as
- exchanging information on national legislation, information and communication technology (ICT) security strategies, policies and best practices.

Further to this, the UN GGE in 2013[5] and 2015[6] recommended states consider a range of confidence building measures described in the following table.

4 https://undocs.org/en/A/65/201
5 http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf
6 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

Confidence Building Measures at UN GGE	
Year	Measure
2013	The exchange of views and information on a voluntary basis on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international co-operation. The extent of such information will be determined by the providing states. This information could be shared bilaterally, in regional groups or in other international forums.
2013	The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from state use of ICTs and how these incidents might develop and be managed.
2013	Enhanced sharing of information among states on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyze and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms.
2013	Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels.
2013	Increased co-operation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among states against disruptions perpetrated by non-state actors.
2013	Enhanced mechanisms for law enforcement co-operation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security.
2015	The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;
2015	The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents

2015	Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security
2015	The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border co-operation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include: (i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies; (ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure; (iii) The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests; (iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.
2015	Strengthen co-operative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions.
2015	Enhance co-operation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations,
2015	Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and co-operation among such national response teams and other authorized bodies,
2015	Expand and support practices in computer emergency response team and cybersecurity incident response team co-operation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector based co-operation
2015	Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

Regional Organisations' efforts on cyber/ICT CBMs

As highlighted above, the UNGGE in its 2015 report in particular provided the groundwork for increased involvement of regional organizations in this space. They have set an initial set of CBMs; however what has become clear since was that regional organizations are uniquely equipped to develop, and in particular implement CBMs. It is easier for them to focus on practical approaches, amongst countries that have common historical and cultural ties, thereby developing the foundational groundwork for enhanced communication, transparency and collaboration. Recent years have seen efforts to do just that at the Organization of American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the Association of South East Asian Nations (ASEAN).

Organization for Security and Co-operation in Europe (OSCE)

Building on its previous success in developing CBMs in the conventional weapons area, the OSCE worked on and adopted two sets of cyber-related confidence-building measures since 2012, when the organization first decided to establish an informal working group to explore a possible OSCE role in strengthening cybersecurity. [7] The latter provided a platform to engage in structured, but still informal, discussions on CBMs. The first set of OSCE CBMs (2013) established official Points of Contact (PoC) and communication lines to prevent possible tensions resulting from cyber activities. [8] The second set (2016) focused on further enhancing co-operation between OSCE participating states: including, for example, effective mitigation of cyberattacks on critical infrastructure. [9]

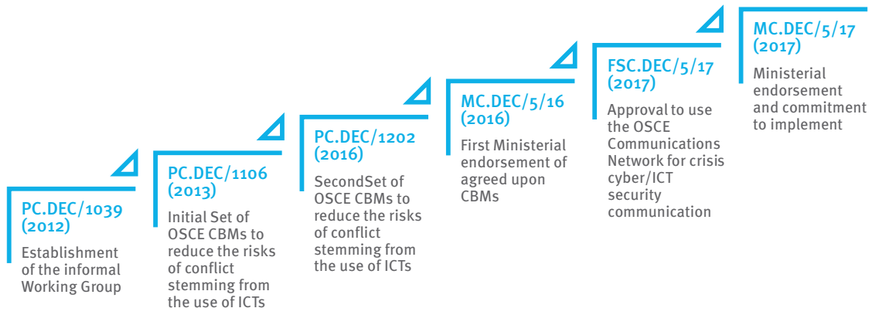


Chart 1: Overview of OSCE CBM-related decisions from 2012 to 2017. [10]

7 OSCE, Permanent Council Decision No. 1039 in 2012, available at: https://www.osce.org/pc/90169
8 OSCE, Permanent Council Decision No. 1106 in 2013, available at: https://www.osce.org/pc/109168
9 OSCE, Permanent Council Decision No. 1202 in 2016, available at: https://www.osce.org/pc/227281
10 "The Role of OSCE Confidence-Building Measures in addressing cyber/ICT security challenges", Nikolas Ott, Central Asian Internet Governance Forum 2019, Plenary session: Using the Internet to strengthen the resilience of the region, Tashkent, Uzbekistan."

The 16 voluntary CBMs can be broadly categorised in three clusters:

- **Posturing CBMs,** which allow States to "read" another State's posturing in cyberspace in order to make cyberspace more predictable;
- **Communication CBMs,** which offer opportunities for timely communication and co-operation, including to defuse potential tensions; and
- **Preparedness CBMs,** which promote national preparedness and due diligence to address cyber/ICT challenges".

Confidence Building Measures at the OSCE		
Year	**Measure**	**Category**
2013	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.	**Posturing**
2013	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.	**Preparedness**
2013	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.	**Communication**
2013	Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.	**Posturing**
2013	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.	**Communication**
2013	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.	**Preparedness**
2013	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.	**Posturing**
2013	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 co-ordinate 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.	**Communication**
2013	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.	**Posturing**
2013	Participating States will voluntary 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.	**Posturing**

2013	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 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/12/682 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.	Communication
2016	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 subregional 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. With respect to such activities participating States are encouraged, inter alia, to: • 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, centres of excellence and civil society in such activities.	Preparedness
2016	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.	Communication
2016	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.	Preparedness

2016	Participating States, on a voluntary basis, will encourage, facilitate and/or participate 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. Collaboration may, inter alia, include: • 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 subregional 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.	Preparedness
2016	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.	Co-operative

Subsequently, the OSCE's focus has shifted from developing additional CBMs towards ensuring that all states properly implement the existing ones through practical support. This includes the use of the OSCE Communications Network "to address security of and in the use of information and communication technologies [...] upon the identification of contact centers/points for cyber/ICT security-related communications within capitals."[11] Several of these initiatives can be seen as complementing and taking forward the work being done at the UN GGE; others however may even generate ideas which have yet to be covered by UN GGE reports.

11 OSCE, FSC.DEC/5/17, Use of the OSCE Communications Network to Support Implementation of Permanent Council Decisions No. 1039, No. 1106 and No. 1202, 19 July 2017, FSC.DEC/5/17, available at: https://www.osce.org/forum-for-security-cooperation/331821?download=true

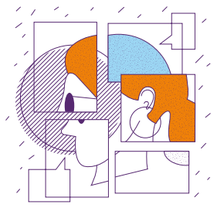
For example, as an effort to increase ownership and targeted implementation, the OSCE launched an "adopt a CBM initiative" within the Informal Working Group in late 2017.

States that formally 'adopt' a CBM bring forward proposals on how to advance its respective implementation, use or impact within the OSCE community. Furthermore, with the purpose of promoting, assisting and fostering the implementation process of existing cybersecurity CBMs, in 2016, the OSCE launched a project that aims to identify and prioritize national implementation challenges. Within this project, it facilitates the creation of national implementation roadmaps and customized capacity-building assistance plans in co-operation with partners, such as the Global Forum on Cyber Expertise (GFCE).

Association of Southeast Asian Nations (ASEAN) and the ASEAN Regional Forum (ARF)

ASEAN has also taken steps in this domain. The ASEAN Regional Forum (ARF) in particular has sought to promote adoption of CBMs since 2012, including through a series of awareness raising workshops. These focused on incident response and regional coordination in particular. Moreover, under Singapore's initiative, the ASEAN Cyber Capacity Program was launched in 2016 to support cyber norms and CBMs in the region.

Prior to that, in 2015, the ARF agreed a work plan on CBMs, and in 2017 launched an open-ended Study Group on Confidence Building Measures[12] to reduce the risk of conflict stemming from the use of ICTs.



The Study Group was tasked with developing processes and procedures for sharing information between ARF contact points on preventing ICT crises, and criminal and terrorist use of ICTs and with the establishment of a contacts database. As a result, through a series of ministerial meetings, norms and CBMs rose to the top of the cyber security agenda, resulting in a formal endorsement of the 11 norms recommended by the UN GGE 2015 report during the ASEAN Ministerial Conference on Cybersecurity (AMCC) in September 2018[13].

12 https://cil.nus.edu.sg/wp-content/uploads/formidable/14/2015-ARF-WP-on-ICT-Security.pdf

13 "The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level", Nikolas Ott and Anna-Maria Osula, 2019, "2019 11th International Conference on Cyber Conflict: Silent Battle", NATO CCD COE Publications, Tallinn. https://ccdcoe.org/uploads/2019/06/Art_18_The-Rise-of-the-Regionals.pdf

Confidence Building Measures at ASEAN Regional Forum	
Year	Measure
2015	the voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations related to security of and in the use of ICTs as well as the procedures for this sharing of information;
2015	discussion exercises involving co-operation among ARF participating countries, on how to prevent incidents related to security of and in the use of ICTs becoming regional security problems;
2015	conduct of surveys on lessons learnt in dealing with threats to the security of and in the use of ICTs and creation of ARF databases on potential threats and possible remedies, taking into account the work that is already done in the commercial computer security sector and in the CERT community in this regard;
2015	capacity building related to security of and in the use of ICTs and to combating criminal use of the internet;
2015	promotion of and co-operation in research and analysis on issues relevant to security of and in the use of ICTs
2015	discussion on rules, norms, and principles of responsible behaviour by ARF Participating Countries and the role of cultural diversity in the use of ICTs;
2015	raising awareness for non-technical personnel and policy makers on threats in the use of ICTs and methods for countering such threats
2015	measures to promote co-operation among ARF Participating Countries against criminal and terrorist use of ICTs including, inter alia, co-operation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional co-operation mechanism
2015	discussion on the terminology related to security of and in the use of ICTs to promote understanding of different national practices and usage;
2015	consideration of establishment of senior policy Point of Contacts between ARF Participating Countries to facilitate real time communication about events and incidents in relation to security of and in the use of ICTs of potential regional security significance; and
2015	consideration of establishment of channels for online information sharing on threats in ICT space, global ICT incidents and sources of ICT attacks threatening critical infrastructure, and development of modalities for real time information sharing (leveraging activities conducted by CERT networks).

Organization of American States (OAS)

OAS launched its efforts to develop CBMs at the First Summit of the Americas in the 1990's, focused on traditional CBMs. Through its resolution AG/RES. 1123 (XXI-O/91), «Co-operation for Security in the Hemisphere,» the General Assembly entrusted the Permanent Council with setting up a working group, with the specific mandate of studying and making recommendations on co-operation on the various dimensions of hemispheric security. As a result of the work of the working group, the General Assembly, in 1993, through resolution AG/RES. 1237 (XXIII-O/93), resolved to convene the first meeting of government experts on confidence- and security-building measures in the Hemisphere, which was held in Buenos Aires, Argentina, in March 1994.[14]

In 2004 it adopted the Comprehensive Inter-American Cybersecurity Strategy encompassing a number of initiatives aimed at strengthening trust between member states, including formation of an inter-American alert, watch, and warning network to rapidly disseminate cybersecurity information and respond to incidents, and developing secure infrastructure for managing sensitive information, enhancing the ability to communicate securely with stakeholders, and establishing procedures to guard against inappropriate disclosure of information.

In 2018, the OAS adopted a resolution stressing the need to prepare and agree upon a set of CBMs for cyberspace to enhance interstate co-operation, transparency, and in turn stability online[15].

The first meeting of the Working Group on Co-operation and Confidence-Building Measures in Cyberspace was and the proposed CBMs were agreed to with a proposed plan of action to establish additional measures. On May 4,2018, member states approved resolution CICTE/RES.1/18 and agreed to the two Regional CBMs to continue the work of the Working Group on Co-operation and Confidence-Building Measures in Cyberspace as a permanent mechanism, and that it continues to meet as needed, in person or by digital means, to discuss new and agreed-upon cyber CBMs. In 2019, the Working Group recommended four (4) new CBMs.

14 https://www.oas.org/csh/english/csbmintro.asp
15 http://www.oas.org/en/sms/cicte/Documents/Sessions/2018/FINAL/RES%201%20Resolución%20Medidas%20Regionales%20de%20Fomento%20CICTE01217E.doc

Confidence Building Measures at OAS

Year	Measure
2017	Establishment of the Working Group on Co-operation and Confidence Building measures in Cyberspace [16]
2018	Member States agreed to provide information on cybersecurity policies, such as national strategies, white papers, legal frameworks, and other relevant documents
2018	Member States agreed to nominate a national point of contact at the policy level able to discuss the implications of hemispheric cyber threats. These points of contact will be distinct from, yet supplement the ongoing work of law enforcement and other technical experts in combating cybercrime and responding to cyber incidents of concern. This information will be updated annually, or as frequently as needed, and shared among partners in a transparent and readily accessible format.
2019	Member States noted with satisfaction at the Nineteenth Session of CICTE, the results of the second meeting of the Working Group, held April 23 and 2019 ,24 in Santiago, Chile, contained in document CICTE/GT/MFCC/doc.19/12 rev. 2 corr. 1 To agree to the four[17] Regional Confidence-Building Measures (CBMs) to Promote Co-operation and Trust in Cyberspace: Designate points of contact, if they do not currently exist, in the Ministries of Foreign Affairs with the purpose of facilitating work for cooperation and international dialogues on cybersecurity and cyberspace. Develop and strengthen capacity building through activities such as seminars, conferences, and workshops, for public and private officials in cyber diplomacy, among others. Encourage the incorporation of cybersecurity and cyberspace issues in basic training courses and training for diplomats and officials at the Ministries of Foreign Affairs and other government agencies. In Summary: 1. They also made recommendations to implement the second measure, that were agreed upon by the Working Group on Co-operation and Confidence-Building Measures in Cyberspace during its second meeting, and include them in the resolution of the Committee on Hemispheric Security that will be transmitted to the forty-ninth regular session of the General Assembly for their inclusion in the "Consolidated List of Confidence- and Security-Building Measures" as non-traditional measures. 2. To continue the work of the Working Group on Co-operation and Confidence-Building Measures in Cyberspace as a permanent mechanism, and that it continues to meet as needed, in person or by digital means, to discuss new and agreed-upon cyber CBMs. 3. To consider the possibility of making voluntary contributions, through CICTE's Cybersecurity Program, to support the work of the Working Group on Co-operation and Confidence-Building Measures in Cyberspace. 4. That the CICTE Secretariat, through its Cybersecurity Program, continue to act as Technical Secretariat for this Working Group and organize its meetings within available financial and human resources.

16 http://www.oas.org/en/sms/cicte/Documents/Sessions/2018/FINAL/RES%201%20Resolución%20Medidas%20Regionales%20de%20Fomento%20CICTE01217E.doc
17 http://scm.oas.org/doc_public/ENGLISH/HIST_17/CICTE01114E07.doc

Other notable international statements on cyber CBMs

In addition to the multilateral and regional initiatives, numerous countries have released specific multilateral and bilateral statements on cybersecurity CBMs. The list that follows is not comprehensive, but highlights a few of the most notable developments in the past few years.

- ### G7 Declaration on Responsible States Behavior in Cyberspace[18]

  - **"We believe that confidence building measures on States' use of ICTs are also an essential element to strengthen international peace and security.**
    We continue to support the development and implementation of such practical CBMs, including communication channels among States for crisis management, in relevant bilateral, regional and multilateral forums, including the Organization for Security and Co-operation in Europe (OSCE) and the ASEAN Regional Forum (ARF);"
  - To increase predictability and stability in cyberspace, we call on States to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible in order to improve transparency and give rise to more settled expectations of State behavior.

- ### G7 Foreign Ministers' Meeting April 10-11, 2016 Joint Communique[19]

  - "We commit to strengthening our co-operation in promoting the rule of law in cyberspace, capacity building, confidence building, and the fight against cybercrime."

- ### G7 Principles and Actions on Cyber[20]

  - "We support the continued development and implementation of cyber confidence building measures between states to promote trust and reduce the risk of conflict stemming from the use of ICTs."
  - "We endeavor to strengthen our co-operation to promote security and stability in cyberspace, including through the promotion of co-operation among national computer security incident response teams, capacity building, and awareness raising. We commit to enhance cybersecurity threat information sharing and to cooperate for improvement of cybersecurity of critical infrastructure such as finance, energy, transportation, and telecommunication."

18 https://www.mofa.go.jp/files/000246367.pdf
19 https://eeas.europa.eu/headquarters/headquarters-homepage/5310_en
20 https://www.mofa.go.jp/files/000160279.pdf

- ### Agreement between the Governments of the Member States of the Shanghai Co-operation Organization on Co-operation in the Field of International Information Security [21]

  - establishing a system to monitor and jointly respond to threats emerging in this area;
  - elaborating and implementing joint confidence-building measures to ensure international information security;
  - " information exchange on legislation of the States of the Parties on issues of ensuring information security"
  - improving the international legal base and practical mechanisms of co-operation among the Parties in ensuring international information security;"
  - "exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized representatives and experts of the Parties in the field of information security;"

- ### NATO Wales Summit Declaration 2014

  - "We are committed to developing further our national cyber defence 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 co-operation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence 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."

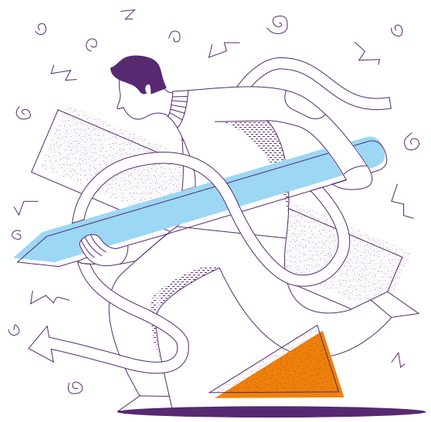
- ### NATO Warsaw Summit Communique 2016[22]

  - "Together with the continuous adaptation of NATO's cyber defense capabilities, this will reinforce the Alliance's cyber defense. We are expanding the capabilities and scope of the NATO Cyber Range, where Allies can build skills, enhance expertise, and exchange best practices. We remain committed to close bilateral and multilateral cyber defense co-operation, including on information sharing and situational awareness, education, training, and exercises. Strong partnerships play a key role in effectively addressing cyber challenges. We will continue to deepen co-operation with the EU, as agreed, including through the on-going implementation of the Technical Arrangement that contributes to better prevention and response to cyber-attacks."
  - "We welcome the work on voluntary international norms of responsible state behavior and confidence-building measures regarding cyberspace."

21 Agreement between the Governments of the Member States of the Shanghai Co-operation Organization on Co-operation in the Field of International Information Security
22 http://www.nato.int/cps/en/natohq/official_texts_133169.html

- **VII BRICS Summit Ufa Declaration**[23]

  - **"In that context, the Working Group of Experts of the BRICS States on security in the use of ICTs will initiate co-operation in the following areas… the establishment of nodal points in member states;"**
  - "In that context, the Working Group of Experts of the BRICS States on security in the use of ICTs will initiate co-operation in the following areas: sharing of information and best practices relating to security in the use of ICTs;"
  - "In that context, the Working Group of Experts of the BRICS States on security in the use of ICTs will initiate co-operation in the following areas… intra-BRICS co-operation using the existing Computer Security Incident Response Teams (CSIRT)."



- **Strengthening Hemispheric Co-operation and Development in Cybersecurity and Fighting Terrorism in the Americas**[24]

  - "The importance of creating frameworks and protocols for co-operation and assistance among the member states, for when incidents occur in one member state and their effects are felt in others; Their commitment to creating confidence-building measures that strengthen international peace and security and that can increase co-operation, transparency, predictability, and stability among states in the use of cyberspace, recognizing confidence and security building measures as one of the lynchpins of collaboration among member states which enhance trust and co-operation and reduce the risk of conflict";
  - "The importance for all the members to create and/or strengthen specialized units within their relevant law enforcement agencies for the prevention and investigation of cybersecurity incidents; Their willingness to provide assistance and training for improving security in the use of information and communications technologies (ICTs), and to share their best technical, legal, and administrative practices to that end; The need to establish procedures for mutual assistance when responding to incidents, in addressing short-term network security problems, and provide collaboration with the reciprocal requests made by the member countries in order to investigate and prosecute crime related to terrorist acts, including procedures for expediting that assistance";
  - "The need for the CICTE Secretariat, within its competencies, in accordance with the 2004 Comprehensive Inter-American Cybersecurity Strategy (the 2004 Strategy and its Appendix A) to continue developing co-operation mechanisms with other international agencies and organizations in order to take coordinated actions for the protection and use of cyberspace;"

23 http://brics2016.gov.in/upload/files/document/5763c20a72f2d7thDeclarationeng.pdf
24 http://brics2016.gov.in/upload/files/document/5763c20a72f2d7thDeclarationeng.pdf

  - "The need for all the member states to continue with their efforts to establish and/or strengthen national alert, monitoring, and response groups for cybersecurity incidents, known as Computer Security Incident Response Teams (CSIRTs); The importance of the member states participating in and strengthening the hemispheric security network of the CSIRTs and cybersecurity authorities, and of the member states increasing their exchanges of information and their co-operation related to the protection of critical information infrastructure and for the prevention of and response to cybersecurity incidents;"

- **Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations**[25]

  - "They provided updates on their respective domestic cybersecurity efforts and discussed the impacts of developments in the European Union, NATO, OSCE, OECD, and the UN, among others."

- **U.S.-Russian Co-operation on Information and Communications Technology Security**[26]

  - "To facilitate the regular exchange of practical technical information on cybersecurity risks to critical systems, we are arranging for the sharing of threat indicators between the U.S. Computer Emergency Readiness Team (US-CERT) located in the Department of Homeland Security, and its counterpart in Russia. On a continuing basis, these two authorities will exchange technical information about malware or other malicious indicators, appearing to originate from each other's territory, to aid in proactive mitigation of threats."
  - "As we work to create predictability and understanding in the political-military environment, both the U.S. and Russian militaries have shared unclassified ICT strategies and other relevant studies with one another."
  - "The White House and the Kremlin have authorized a direct secure voice communications line between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council, should there be a need to directly manage a crisis situation arising from an ICT security incident. This direct line will be seamlessly integrated into the existing Direct Secure Communication System ('hotline') that both governments already maintain, ensuring that our leaders are prepared to manage the full range of national security crises we face internationally".

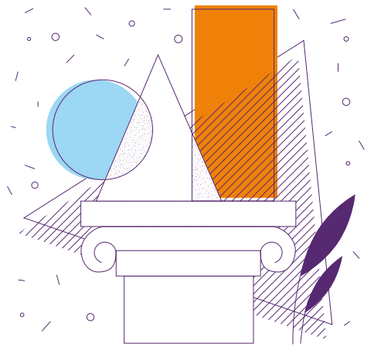
25 https://obamawhitehouse.archives.gov/the-press-office/2016/08/23/joint-declaration-increased-security-and-defense-co-operation-between
26 https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-co-operation-information-and-communications-techno

- **Joint Elements from E.U.-U.S. Cyber Dialogue, 23 December 2016**[27]
  - "Both the European Union and the United States shared information on recent developments to bolster cybersecurity and resilience efforts on both sides of the Atlantic. They elaborated on the European Union's Network Information Security directive to be implemented across Member States and the conduct of the CyberEurope 2016 exercise. They also discussed the second iteration of the Cybersecurity Framework for voluntary standards, including continued stakeholder engagement and adoption of the framework, as well as the new U.S. National Cyber Incident Response Plan and its "severity schema" for planning and preparedness purposes. The two sides agreed to continue to share information about these and other efforts on an on-going basis and coordinate on such efforts."

- **First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes**[28]
  - "Hotline Mechanism. Pursuant to the commitment between the two presidents to establish a hotline for escalation of issues that may arise in the course of responding to cybercrime and other malicious cyber activities, both sides decided to develop the scope, goals and procedures for use of the hotline before the next High-Level Dialogue."

- **Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group**[29]
  - "[I]n the event of a serious cyber incident that threatens the security of either of our nations, including if such a cyber incident occurs as a part of an armed attack against Japan, the MOD and DOD will consult closely and take appropriate co-operative actions. In particular, the DOD will consult with the MOD and support Japan via all available channels, as appropriate."

- **Australian international cybersecurity strategy**[30]
  - "Australia is committed to taking practical action to support international peace and security. Confidence building measures foster trust between states to prevent misunderstandings that could lead to conflict. They include transparency measures, risk reduction measures and co-operative measures.
    Confidence building measures are one of the most important tools in our diplomatic toolkit.
    Australia is committed to implementing these measures to maintain a peaceful and stable online environment".



27 https://web.archive.org/web/20170113041119/https:/www.state.gov/r/pa/prs/ps/2016/12/265970.html
28 https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0
29 http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf
30 https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_4_international_security_and_cyberspace.html

Bibliography

VII BRICS Summit, Ufa Declaration, 2015
http://brics2016.gov.in/upload/files/document/5763c20a72f2d7thDeclarationeng.pdf

Australian international cybersecurity strategy, 2018
https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_4_international_security_and_cyberspace.html

Building Confidence in the Cybersphere: A Path to Multilateral Progress, Theresa Hitchens and Nancy W. Gallagher, 2018 https://www.cissm.umd.edu/sites/default/files/Building%20Confidence%20in%20the%20Cybersphere%20-%20final%20version%20-%20070918.pdf

Confidence Building Measures and International Cyber Security, Daniel Stauffacher, 2013
https://ict4peace.org/wp-content/uploads/2015/04/processbrief_2013_cbm_wt-71.pdf

Confidence-Building Measures in Cyberspace A Multistakeholder Approach for Stability And Security, Atlantic Council, 2014
http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

Confidence Building for Cybersecurity between China and the United States, Dong Qingling, 2014
http://www.ciis.org.cn/english/2014-09/23/content_7254470.html

Confidence Building Measures for the Cyber Domain, Strategic Studies Quarterly, Erica D. Borghard and Shawn W. Lonergan, 2018
https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Borghard-Lonergan.pdf

CyberNorms Index, Carnegie Endowment for International Peace
https://carnegieendowment.org/publications/interactive/cybernorms

Cybersecurity Tech Accord: "Promoting international peace and stability by building trust between states in cyberspace: The importance of effective confidence-building measures"
https://cybertechaccord.org/uploads/prod/2019/04/FINALOASWP.pdf

Cybil portal
https://cybilportal.org/

Delhi Communique, 2017
https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique

European Parliament briefing: Cyber diplomacy: Confidence-building measures, 2015
http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS_BRI(2015)571302_EN.pdf

First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes, 2015
https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0

G7 Foreign Ministers' Meeting April 10-11, 2016 Hiroshima, Japan Joint Communiqué
https://www.mofa.go.jp/files/000160279.pdf

G7 declaration on responsible states behavior in cyberspace, 2017
https://www.mofa.go.jp/files/000246367.pdf

G7 Foreign Ministers' MeetingJoint Communiqué, 2016
http://eeas.europa.eu/statements-eeas/2016/160411_02_en.htm

Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group May 30, 2015
http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf

Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations, 2016
https://web.archive.org/web/20170105211311/https:/www.state.gov/r/pa/prs/ps/2016/09/262038.htm

Joint Elements" from the EU-U.S. Cyber Dialogue, 2016
https://web.archive.org/web/20170113041119/https:/www.state.gov/r/pa/prs/ps/2016/12/265970.htm

Organization of American States, Confidence and security-building measures
https://www.oas.org/csh/english/csbmintro.asp

Organization of American States, Resolution on regional confidence-building measures to promote cooperation and trust in cyberspace, 2018
http://www.oas.org/en/sms/cicte/Documents/Sessions/2018/FINAL/RES%201%20Resolución%20Medidas%20Regionales%20de%20Fomento%20CICTE01217E.doc

Organization of American States, Establishment of a working group on cooperation and confidence-building measures in cyberspace, 2017
http://scm.oas.org/doc_public/ENGLISH/HIST_17/CICTE01114E07.doc

Organization of American States, Resolution on Regional confidence-building measures to promote cooperation and trust in cyberspace, 2019
http://scm.oas.org/doc_public/ENGLISH/HIST_19/CICTE01297E03.doc

OSCE Guide on Non-military Confidence-Building Measures (CBMs), 2012
https://www.osce.org/secretariat/91082?download=true

OSCE, Permanent Council Decision No. 1039, 2012
https://www.osce.org/pc/90169

OSCE, Permanent Council Decision No. 1106, 2013
https://www.osce.org/pc/109168

OSCE, Permanent Council Decision No. 1202,2016
https://www.osce.org/pc/227281

"The Role of OSCE Confidence-Building Measures in addressing cyber/ICT security challenges", Nikolas Ott, Central Asian Internet Governance Forum 2019, Plenary session: Using the Internet to strengthen the resilience of the region, Tashkent, Uzbekistan."
https://cil.nus.edu.sg/wp-content/uploads/formidable/14/2015-ARF-WP-on-ICT-Security.pdf

The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level", Nikolas Ott and Anna-Maria Osula, 2019, "2019 11th International Conference on Cyber Conflict: Silent Battle", NATO CCD COE Publications, Tallinn.
https://ccdcoe.org/uploads/2019/06/Art_18_The-Rise-of-the-Regionals.pdf

Warsaw Summit Communiqué, 2016
http://www.nato.int/cps/en/natohq/official_texts_133169.htm

UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security report, 2010
https://undocs.org/en/A/65/201

UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security report, 2013
http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf

UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security report, 2015
http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174