International Cyber Norms:
Legal, Policy & Industry Perspectives,
Anna-Maria Osula and Henry Rõigas (Eds.),
NATO CCD COE Publications, Tallinn 2016

CHAPTER 7

Confidence-Building Measures in Cyberspace: Current Debates and Trends

Patryk Pawlak

1. Introduction

The rapidly shifting global digital environment is raising concerns about the sustainability of the positive contribution that the Internet has made towards economic and human development.[1] Since the end of the 1990s, when the debate about the impact of information and communication technologies on international security was first raised on the international agenda, the number of Internet users has grown over a thousand-fold from just 3 million in 1990 to over 3.2 billion in 2015 and is expected to reach 4.7 billion by 2025.[2] Most of this growth will continue to come from developing countries, including countries in Asia and Africa. The number of mobile devices is already higher than the world's population.[3] Digital environment and threat landscape are changing too: state and non-state actors increasingly exploit vulnerabilities in cyberspace to gain advantage over their competitors and adversaries.[4] The assessment of national cyber security programmes conducted by UNIDIR in 2012 has shown that an increasing number of states give some role to the armed forces.[5] Research also shows that out of 15 largest military spenders, 12

1 Patryk Pawlak, ed., European Union, Institute for Security Studies, *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development*, Report No. 21 (December 2014), http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf.

2 David Burt, et al, Microsoft, *Cyberspace 2025. Today's Decisions, Tomorrow's Terrain. Navigating the Future of Cybersecurity Policy* (June 2014).

3 CISCO, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014-2019: White Paper* (3 February 2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

4 Symantec, *The 2015 Internet Security Threat Report (ISTR20)*, vol. 20 (April 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

5 James Andrew Lewis and Götz Neuneck, *The Cyber Index: International Security Trends and Realities* (New York and Geneva: United Nations Institute for Disarmament Research, 2013), http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

are developing dedicated cyber warfare units and two-thirds appear to possess or be developing offensive cyber capabilities.[6]

As Internet-based platforms and infrastructure continue to grow in importance for the delivery of basic services and become part of critical national infrastructure, the risk of conflict resulting from misunderstandings or misperceptions between countries becomes more acute. To reduce the possibility of such a scenario materialising, the international community has engaged in several regional or global processes focused on clarifying how the existing international law applies to cyberspace, development of norms of responsible state behaviour, and development of confidence-building measures (CBMs). The overarching link for these efforts has been provided by four consecutive United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGEs). However, there is a growing concern that the concepts, methods and measures developed by various regional and international forums may evolve in diverging directions further contributing to uncertainty.

The aim of this chapter is to investigate the evolution of confidence-building measures in cyberspace, their features, main trends, and possible trajectories for development in the future. Even though building confidence in cyberspace is a process that requires the involvement of all layers of society – as demonstrated by a large breadth of contributions in this volume – this chapter investigates solely the evolution of confidence-building measures between states and state institutions at bilateral, regional or international level.[7] However, the chapter also notes the increasing focus on capacity-building in strengthening the implementation of CBMs. The chapter concludes with the presentation of two distinct models illustrating how norms, CBMs and capacity-building contribute to stability in cyberspace.

2. Uncertainty in Cyberspace

With cyber security attracting increasing interest and the barriers for access to cyber capabilities decreasing, the risk of a conflict resulting from misunderstandings and miscalculation is also growing. The reliance on ICT platforms for delivery of government, financial and public services makes their users vulnerable to cyber attacks by organised criminal groups or foreign governments.

Because cyberspace enables certain levels of anonymity, state, state-sponsored and non-state actors do not shy from exploiting these vulnerabilities. The first report of the UN GGE delivered in 2010 stressed that 'uncertainty regarding attribution and the absence of common understanding regarding acceptable state behaviour may create the

6 Ibid.
7 See chapters 10, 11 and Appendix 1 for private sector perspectives.

risk of instability and misperception.'[8] The difficulties with attribution of attacks give states the ability to deny responsibility,[9] as has been the case for the North Korean government which has consistently denied any involvement in the cyber attacks on Sony Pictures Entertainment.[10] The challenges related to attribution are even more daunting if one takes into account the possible consequences of an erroneous attribution and a relatively easy access to instruments for conducting cyber attacks by cyber criminals and hackers. For instance, the cyber attacks against TV5 Monde initially attributed to ISIL/Da'esh were later re-attributed to attackers based in Russia.[11] On the other hand, malware discovered on the Nasdaq servers in 2014 was initially assessed as originating from the Russian Federal Security Service and capable of destroying the content of the entire stock exchange; it was subsequently found to be less destructive and planted by two Russian hackers.[12]

The protection of cyberspace and reducing its vulnerability to digital threats has become a key element of national security strategies. While a substantial part of the adopted solutions are of non-military nature (legislation, organisational adaptation and training), many countries have been also investing in offensive and defensive cyber capabilities of military nature.[13] The risk is, however, that the progressing militarisation of cyberspace and the reliance on new systems of state-owned cyber weapons[14] similar to *Red October*, *Flame*, *Duqu* or *Stuxnet* will accelerate the cyber arms race, and competition for 'digital supremacy'[15] ultimately increasing the risk of escalation and conflict. Militarisation and expansion of cyber weapons is also problematic due to the ambiguity concerning qualification of a cyber attack as a use of force under Article 2(4) of the UN Charter, and the threshold for self-defence as stipulated in Article 51.[16] Establishing whether a cyber attack constitutes an armed attack, if the use of force is legitimate (*jus ad bellum*), and how force can be employed (*jus in bello*) is still a subject of a debate among international legal scholars and policymakers.[17]

8 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 July 2010), http://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf.

9 Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38 (2014): 4-37, https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf.

10 David E. Sanger and Nicole Perlroth, 'U.S. Said to Find North Korea Ordered Cyber Attack on Sony,' *The New York Times*, December 17, 2014, http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0; 'NorthKorea Proposes Joint Sony Hack Inquiry with US,' *BBC News*, December 20, 2014, http://www.bbc.com/news/world-us-canada-30560712.

11 Adam Thomson, 'ISIS Hackers Cut Transmission of French Broadcaster,' *Financial Times*, April 9, 2015, http://www.ft.com/cms/s/0/5f419994-de94-11e4-8a01-00144feab7de.html#axzz3wSJjk22o; 'APT28: A Window into Russia's Cyber Espionage Operations?' *FireEye*, October 27, 2014, https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

12 Benjamin Brake, *Strategic Risks of Ambiguity in Cyberspace*, *Contingency Planning Memorandum No. 24* (Council on Foreign Relations, 2015), http://www.cfr.org/cybersecurity/strategic-risks-ambiguity-cyberspace/p36541.

13 Lewis and Neuneck, *The Cyber Index: International Security Trends and Realities.*

14 Gary D. Brown and Andrew O. Metcalf, 'Easier Said than Done: Legal Reviews of Cyber Weapons,' *Journal of National Security Law and Policy* 7 (2014): 115-138, http://jnslp.com/wp-content/uploads/2014/02/Easier-Said-than-Done.pdf.

15 Kenneth Geers, et al, FireEye, *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks* (2014), https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf.

16 The UN General Assembly Resolution 3314 (XXIX) defines aggression as 'the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations.' UN General Assembly resolution 3314 (XXIX), *Definition of Aggression*, 3314 (XXIX) (14 December 1974), http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement. See also Michael N. Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context,' in *4th International Conference on Cyber Conflict: Proceedings*, eds. Christian Czosseck, Rain Ottis and Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2012).

17 See: Schmitt, '"Attack" as a Term of Art in International Law.'; Michael N. Schmitt, 'Classification of Cyber Conflict', *Journal of Conflict and Security Law* 17 (2012): 245-260, http://jcsl.oxfordjournals.org/content/17/2/245.full; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

3. Confidence-Building Measures and Norms: Two Sides of the Same Coin

Confidence-building measures are one of the key mechanisms in the international community's toolbox aiming at preventing or reducing the risk of a conflict by eliminating the causes of mistrust, misunderstanding and miscalculation between states.[18] Most of the existing confidence-building measures date back to 1975 when the Helsinki Final Act[19] was adopted, followed by the 1986 Stockholm Document on Confidence- and Security-Building Measures and Disarmament in Europe,[20] and the 1990 Vienna Document.[21] Military confidence-building measures aim to prevent a potential outbreak of military conflict by improving relations between government officials and militaries.[22] Their primary focus is on increasing transparency, improving information exchanges, and restraining the use of violence by armed forces. The assumption is that exchange of information about military doctrines and resources contributes to stability by enhancing situational awareness and building common understandings. However, while CBMs can contribute to de-escalating an unintended conflict, they are of limited use when conflicts are fuelled intentionally.

The reports on the implementation of United Nations General Assembly Resolution 65/63 of 2011 concerning information on confidence-building measures in the field of conventional arms indicate three main categories of military CBMs: communication and information exchange measures; transparency and verification measures; and military restraint measures.[23] Non-military confidence-building measures are used to preserve peace by building trust between communities, including law enforcement, incident responders, or civil society, through actions or processes undertaken across political, economic, environmental, social or cultural fields.[24] Both have a number of objectives in common: to prevent armed conflict; limit violence; and ideally provide foundations for sustainable

18 Daniel Stauffacher, ed. and Camino Kavanagh, rap., ICT4Peace Foundation, *Confidence Building Measures and International Cyber Security: Cyber Policy Process Brief* (2013), http://ict4peace.org/wp-content/uploads/2015/04/processbrief_2013_cbm_wt-71.pdf.

19 'Conference on Security Co-operation in Europe: Final Act' (Organization for Security and Co-operation in Europe, Conference on Security Co-operation, Helsinki, 1975), https://www.osce.org/mc/39501?download=true.

20 'Document of the Stockholm Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-operation in Europe' (Organization for Security and Co-operation in Europe, 19 September 1986), https://www1.umn.edu/humanrts/peace/docs/stockholm1986.html.

21 'Vienna Document 1990 of the Negotiations on Conference on Confidence and Security Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Vienna Meeting of the Conference on Security and Co-operation in Europe' (Organization for Security and Co-operation in Europe, Vienna, 17 November 1990).

22 United Nations, General Assembly, *Special Report of the Disarmament Commission to the General Assembly at Its Third Special Session Devoted to Disarmament*, A/S-15/3 (28 May 1988), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/S-15/3%28SUPP%29&Lang=E.

23 United Nations, General Assembly, *Information on Confidence-Building Measures in the Field of Conventional Arms: report of the Secretary-General*, A/66/176 (25 July 2011), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/429/12/PDF/N1142912.pdf?OpenElement.

24 'OSCE Guide on Non-Military Confidence-Building Measures (CBMs)' (Organization for Security and Co-operation in Europe, Vienna, 2012), http://www.osce.org/cpc/91082?download=true.

cooperation. However, developed in an entirely different context – namely to build confidence with regard to the proliferation and use of conventional weapons – the traditional approach to military and non-military CBMs requires certain adaptations in order to adequately reflect the specificity of the digital domain (Table 1).

The discussion about confidence-building measures in cyberspace is closely linked to the parallel debates about acceptable norms of state behaviour. While the focus on norms, both in the existing international law and non-binding political agreements, helps to establish international level of expectations about states' behaviour in cyberspace, development of CBMs provides practical tools to manage these expectations.[25] For instance, the norm according to which states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs creates an expectation that states will use all instruments at their disposal to prevent such unlawful acts from occurring. Hence, it creates a concrete expectation among states. However, such expectations need to be adjusted, taking into account the capacities of individual states to meet their obligations. Confidence-building measures facilitate such adjustments, for example through establishing channels of communication, information exchange and practical cooperation during investigations. The UN GGE 2015 report, for instance, stipulates that 'in case of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences'. Confidence-building measures focusing on transparency and communication provide the necessary foundation for operationalisation of this norm. Without confidence-building measures in place, even legally binding norms enshrined in international treaties only provide an illusion of stability and normalcy.

Differences in the interpretation of the UN GGE 2015 report despite an agreement on a concrete set of norms, also show that there is still certain level of uncertainty which, if not addressed, may contribute to escalation of a conflict.[26] For instance, the report contains a compromise on the use of Article 51 of the UN Charter which gives states the right to individual or collective self-defence in case of armed attacks.[27] However, according to the Russian special envoy for international cooperation in information security, Andrei Krutskikh, 'there is no general idea in the world today what is meant by the 'armed attack' in relation to the use of ICTs'.[28]

25 For a detailed analysis of legal aspects of CBMs, see Katharina Ziolkowski, *Confidence Building Measures for Cyberspace - Legal Implications* (Tallinn: NATO CCD COE Publications, 2013), https://ccdcoe.org/publications/CBMs.pdf.

26 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

27 The compromise language reached in the UNGGE does not make a specific reference to Article 52 of the UN Charter but to the Charter in its entirety. United Nations, General Assembly, *Group of Governmental Experts*, A/70/174.

28 'UN Cybersecurity Report Compromises on Self-Defence Issue – Russian Official,' *Sputnik International*, August 17, 2015, http://sputniknews.com/politics/20150817/1025819426/UN-cybersecurity-report-compromises-on-self-defence.html.

Table 1. Traditional CBMs and cyber-related adaptations.[29]

Aim of a measure	Examples	Suitability in cyberspace
Communication and information exchange measures		
Enhancing mutual understanding of national military capabilities and activities through facilitating regular communication	Military points of contact, hotline between chiefs of the armed forces, exchange of military information on national forces and armaments, advance notification of important military exercises	Feasible but require a clear definition of 'cyber military capabilities' and clear separation of military and civilian capabilities
Transparency and verification measures		
Monitoring of military facilities and activities, primarily in order to ensure that a party's military activities are of a non-aggressive nature	Inviting observers to monitor major military exercises, verification missions on-site	Difficult to implement given the dual-nature of cyber-tools and countries' interest in preserving strategic ambiguity concerning their capabilities
Military restraint measures		
Limiting the capacity of parties for (surprise) offensive military attacks	Restrictions on major military exercises, limitations of troop movements, demilitarised and weapon-free zones	Difficult given the civil-military nature of Internet and lack of transparency. Requires a definition of 'weapon-free zones' in cyberspace in terms of ICT infrastructure and not necessarily linked to geography
Political measures		
Strengthening the confidence in the political system	Power sharing arrangements, proportional recruitment for state and regional institutions, electoral reforms, or decentralisation of power	Feasible through non-discriminatory legislative frameworks, respect for norms, rule of law and human rights; clear division of competences and institutions in place; national cyber security strategy
Economic measures		
Reducing the risk of a conflict through increasing trade and economic interdependency	Trade agreements, customs areas	Feasible through export control mechanisms and increasing dependence on cyberspace for economic growth and development
Environmental measures		
Providing incentives for cooperation in the areas of crisis/disaster management or management of resources	Concrete cooperative measures addressing natural hazards: earthquakes, floods, fires	Feasible through concrete cooperative measures in case of cyber incidents, i.e. CERT-to-CERT
Societal and cultural measures		
Strengthening ties between communities or nations	People-to-people dialogues and joint projects (i.e. exchanges of students)	Feasible through ensuring open access to the Internet, in particular social media but also online services

29 Author's compilation based on Lewis and Neuneck, *The Cyber Index: International Security Trends and Realities.*

It is also important to understand that international law, even though legally binding and applicable to cyberspace, is not a silver bullet for solving the challenges linked to uncertainty in cyberspace. The UN GGE 2013 report reaffirmed that 'international law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment'.[30] However, successive reports have acknowledged the need to better understand how this should be done in practice. CBMs contribute to this process by establishing certain foundations for the debate. They serve as tools for ensuring that states have the same understanding of the normative commitments that they made and are bound to respect. For instance, they may serve as socialisation venues through which actors exchange information about mutual expectations, practices, and working methods, which in turn influences the level of trust and the commitment to certain normative frameworks. Consequently, the processes of development of norms and CBMs are closely linked and interdependent. If norms serve as a certain ideal of behaviour that states aspire to, an adequate mix of CBMs – ranging from those improving situational awareness to building resilience and facilitating cooperation – is supposed to help states achieve them (see Table 2).

In addition, whereas CBMs can prevent unintentional conflicts by stopping or slowing down the spiral of escalation, their usefulness is limited in case of intentional conflict and escalation. Consequently, achieving the full potential of confidence-building measures to minimise misperceptions may be limited by a number of factors that undermine credibility of the parties involved: a limited political will and commitment to preventing a conflict, such as a threat to resort to offensive capabilities as opposed to law enforcement and other alternative approaches; distribution of resources by investment in defence rather than resilience and skills; a weak legal system, such as ineffective rule of law and administration of justice; or recurring hostilities such as cyber attacks.

4. How Do States Build Confidence in Cyberspace?

The foundations for the discussion about the confidence-building measures in cyberspace have been laid down by successive UN GGE reports and quickly became part of the effort undertaken within regional organisations in Europe, the Americas and Asia, albeit with a different focus and results.

4.1 United Nations

Even though United Nations does not work on developing specific CBMs, leaving this task to regional organisations, the initiatives undertaken at the UN level shape a common understanding of the role of CBMs within a larger debate about stability in

30 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 June 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

cyberspace. The issue of information security in the international context was introduced to the United Nations agenda by Russia in 1998.[31] 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 analyse international legal provisions relating to various aspects of international information security and study existing concepts and approaches.[32] The group was convened for the first time in 2004[33] but was not able to reach consensus on the final report due to the 'complexity of the issues involved'.[34] The UN GGE 2010 report further highlighted the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to state use of ICTs, which could affect crisis management in the event of major incidents, and called for new measures, including to 'build confidence, reduce risk and enhance transparency and stability'.[35] The UN GGE 2013 report went further in stating that 'voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception'.[36]

The real breakthrough came with the most recent report of the Governmental Group of Experts established in 2014.[37] The UN GGE 2015 report recommends that, consistent with the purposes of the United Nations, states '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 pose threats to international peace and security'.[38] It reiterates some of the measures suggested in the earlier report but also pays particular attention to measures aimed at reducing the risks of misperceptions and conflicts linked to the attacks on ICT-enabled infrastructure (Table 3). The catalogue of CBMs proposed in the UN GGE 2015 report supplements the consensus achieved in the Organization for Security and Co-operation in Europe (OSCE)[39] and, even though not formally adopted by governments, remains the most comprehensive set of such measures to date. It provides a framework that can be adapted by regional organisations taking into account their specific regional context.

---

31 United Nations, General Assembly resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/53/70 (4 January 1999), http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70.

32 United Nations, General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/58/373 (17 September 2003), https://ccdcoe.org/sites/default/files/documents/UN-030917-ITISreply.pdf.

33 United Nations, General Assembly resolution 58/32, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/58/32 (18 December 2003), https://ccdcoe.org/sites/default/files/documents/UN-031208-ITIS_0.pdf.

34 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/60/202 (5 August 2005), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/453/63/PDF/N0545363.pdf?OpenElement.

35 United Nations, General Assembly, *Group of Governmental Experts*, A/65/201.

36 United Nations, General Assembly, *Group of Governmental Experts*, A/68/98.

37 United Nations, General Assembly resolution 68/243, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/68/243 (9 January 2014), http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015-a-res-68-243-eng-0-589.pdf.

38 United Nations, General Assembly, *Group of Governmental Experts on Developments*, A/70/174.

39 Many of the experts representing states in the UN GGE are also involved in the negotiations of the CBMs in the framework of the OSCE.

4.2 Organization for Security and Co-operation in Europe

Despite its diverse membership, with 57 states from Europe, North America and Asia, OSCE has been spearheading the only project formally endorsed by states aimed at development and implementation of CBMs. The need to address cyber security concerns was recognised for the first time in the OSCE declarations and resolutions adopted in 2008 in Astana,[40] and in 2010 in Oslo.[41] The 2011 Belgrade Declaration called on the international community 'to increase cooperation and information exchange in the field of cyber security, to agree on specific measures to counter the cyber threat and to create, where possible, universal rule of conduct in cyberspace'.[42] In 2012, the OSCE Permanent Council decided to establish an open-ended and informal OSCE working group tasked with elaboration of 'a set of draft confidence-building measures 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'.[43]

The first meeting of the OSCE's Informal Working Group on CBMs related to ICT (IWG-CBM) was convened under the chairmanship of the United States (US). The meeting focused on over 50 proposals for CBMs put forth by various participating states.[44] A short paper presented by the chair focused on three main types of measures: a) enhancing basic confidence and predictability through transparency- and confidence-building measures; b) co-operative methods of crisis prevention and resolution in the event of discrete disruptive activities of non-state actors; and c) stability measures where participating states refrain from destabilising activities in cyberspace and engage in stabilising behaviour. A proposal for a Ministerial Council decision on CBMs to reduce the risks of conflict stemming from the use of ICT was tabled at the 2012 Ministerial Council in Dublin but no decision was adopted due to Russia's objections. Following this failure, the Istanbul Declaration of 2013 urged the OSCE to 'develop confidence-building measures to reduce the risk of cyber conflicts and to promote a culture of cyber security'.[45] On the basis of this political guidance, the OSCE launched the process aimed at the adoption of a set of CBMs. A historical compromise on a set of eleven voluntary CBMs in

40 'Astana Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Seventeenth Annual Session' (Organization for Security and Co-operation in Europe, Seventeenth Annual Session, Astana, 29 June to 3 July 2008), https://ccdcoe.org/sites/default/files/documents/OSCE-080703-AstanaDeclarationandResolutions.pdf.

41 'Oslo Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Nineteenth Annual Session' (Organization for Security and Co-operation in Europe, Nineteenth Annual Session, Oslo, 6-10 July 2010), https://ccdcoe.org/sites/default/files/documents/OSCE-100710-OsloDeclarationandResolutions.pdf.

42 'Belgrade Declaration of the OSCE Parliamentary Assembly and Resolution Adopted at the Twentieth Annual Session' (Organization for Security and Co-operation in Europe, Twentieth Annual Session, Belgrade, 6-10 July 2011), https://www.oscepa.org/documents/all-documents/annual-sessions/2011-belgrade/declaration-4/3024-belgrade-declaration-eng/file.

43 'Decision No. 1039: On development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,' PC.DEC/1039 (Organization for Security and Co-operation in Europe, Permanent Council, 909th Plenary Meeting, 26 April 2012).

44 'Follow-Up on Recommendations in the OSCE PA's Monaco Declaration: Final Report for the 2013 Annual Session' (Organization for Security and Co-operation in Europe, General Committee on Political Affairs and Security, 2013), https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/follow-up-report-3/1782-2013-annual-session-follow-up-final-report-1st-committee-english/file.

45 Istanbul Declaration and Resolution Adopted by the OSCE Parliamentary Assembly at the Twenty-Second Annual Session (Organization for Security and Co-operation in Europe, Twenty-Second Annual Session, Istanbul, 29 June to 3 July 2013), https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/declaration/1801-istanbul-declaration-eng-1/file.

Table 2. Linking norms, CBMs and capacity-building.[46]

NORMS	
Norms, rules and principles of responsible behaviour (UN GGE 2015 Report)	**Challenges to implementation**
In case of ICT incidents, states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.	Highly dependent on political agenda and uncertainty. CBMs are useful tools in creating 'positive expectations' and good faith where doubts exist.
States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.	Proving if a country has known about such acts from their territory is difficult. CBMs help to determine if this is the case.
States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.	Such cooperation is usually based on law enforcement cooperation treaties and relatively easy to monitor. Political will might be an obstacle to implementation that needs to be addressed with CBMs.
States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as UNGA resolutions 68/167 and 69/166 on the right to privacy in the digital age.	Relatively easy to verify with regard to freedom of expression but more complicated with regard to protection of privacy online. CBMs can help improve overall climate for cooperation.
States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.	This statement leaves untouched activities by non-governmental entities of which governments may be aware but not actively support. CBMs can help clarify state's position and demonstrate good faith.
States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account UNGA resolution 58/199 on the creation of a global culture of cyber security and the protection of critical information infrastructures, and other relevant resolutions.	Some countries may not have resources to implement concrete legal or technological solutions and be more vulnerable. In such cases capacity-building amounts to an important CBM.
States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.	In practical terms, such requests can be subjected to extended wait-times and undermine position of the addressee country. CBMs can help clarify reasons for possible delays or missing information.
States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.	These are often difficult to verify. CBMs like export controls and transparency measures – including cooperation among private sector – can be useful way for diffusing potential tensions.
States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.	These are relatively easy to implement through CBMs, if there is enough political will. CBMs at operational level can be more successful.
States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams of another State. A State should not use authorised emergency response teams to engage in malicious activity.	May be difficult to prove and hence CBMs – both at political and operational level – can help clarify the context and resolve conflicts.

46 Author's compilation on the basis of 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures,' PC.DEC/1106; United Nations, General Assembly, *Group of Governmental Experts*, A/70/174.

		CONFIDENCE-BUILDING MEASURES	CAPACITY-BUILDING
		Applicable measures (UN GGE 2015 and OSCE)	**Corresponding capacity-building needed**
	Facilitating cooperation	· Facilitation of cooperation between relevant national bodies (OSCE and UN GGE)	· Competent institution responsible for cyber security policy · Establishing clear division of labour within national administration
	Improving situational awareness	· Sharing information on national organisation, strategies, policies and programmes (OSCE and UN GGE) · Providing a list of national terminology and definitions related to ICT security (OSCE)	· National cyber security strategy and legislation · Cyber procedures: technical, administrative and procedural measures to protect systems · Public-private partnerships
	Protection of critical ICT infrastructure	· Consultations to prevent political and military tensions and protect critical national ICT infrastructure (OSCE and UN GGE) · Sharing information on categories of infrastructure considered critical and facilitating cross-border cooperation to address their vulnerabilities (UN GGE)	· Risk assessment · Developing standards · Public-private partnerships
	Fight against cyber crime	· Put in place modern and effective legislation to facilitate cooperation and effective cross-border cooperation to fight cyber crime and terrorist use of ICTs (OSCE)	· Substantive and procedural laws, criminalisation of certain acts, respect for fundamental freedoms · Sustainable and scalable training for law enforcement, judges and prosecutors · Forensics · Formal and informal channels of communication
	Building resilience	· Providing contact data of existing national structures that manage ICT-related incidents (OSCE and UN GGE) · Development of focal points for the exchange of information on malicious ICT use and provision of assistance in investigations (UN GGE)	· Computer Emergency Response Teams (CERTs) · 24/7 points of contact · Common protocols for sharing information regarding cyber events

cyberspace was contained in Decision 1106 adopted in December 2013 (see Table 3).[47] Participating states may inquire about individual submissions by direct dialogue with the submitting state or during meetings of the Security Committee and IWG-CBMs.

The OSCE 'master plan' is implemented in three stages:

- *Adoption of transparency measures* such as establishing crisis communication mechanisms, and promoting diligence and resilience, as well as exchange of information about national policies and structures. To date, around 40 participating states have implemented one or more of the CBMs adopted in OSCE Decision 1106.[48] Most actions have been focused on sharing information about approaches to cyber security, national cyber and ICT security architectures and international engagement linked to agreed measures.
- *Development of cooperative measures* like assistance in building resilience and other capacity-building initiatives that would strengthen the collective capacity to deal with the cyber threat. Such measures might focus on the development of national security strategies, assistance with establishing Computer Emergency Response Teams (CERTs), or putting in place effective legislation. According to the officials involved in the process, Russia has raised reservations on a number of issues raising the argument that the mandate of the OSCE does not include capacity-building. Contrary to initial expectations, the 21st OSCE Ministerial Council held in December 2015 has failed to reach a compromise on the language, and negotiations over the second set of CBMs will continue throughout 2016 during the German Chairmanship of OSCE.
- *Adoption of stability measures* focused on strengthening states' commitment to refrain from certain types of destabilising activities. Observers agree that this stage will be most difficult to complete as it involves a high level of trust and commitment between the participating states.

As part of the process, the Swiss and Serbian OSCE Chairmanships hosted several workshops on the issue with the aim to take stock of the implementation of the adopted measures, to support the negotiation of a second set of CBMs, and to provide a platform for discussion between non-governmental stakeholders such as critical infrastructure operators. On the basis of the recommendations of the Swiss Showcase Event 2014, OSCE managed to advance the implementation of Decision 1106, in particular with regard to ensuring appropriate channels for consultation, building a network of cyber focal points, and expanding cooperation in the framework of the CBM process to other stakeholders.

47 '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,' PC.DEC/1106 (Organization for Security and Co-operation in Europe, Permanent Council, 975th Plenary Meeting, 3 December 2013), http://www.osce.org/pc/109168?download=true.

48 Michele Coduri, speaker, 'Session I – Promoting the Implementation of the First Set of CBMs' (OSCE Chairmanship Event on Effective Strategies to Cyber/ICT Security Threats, Belgrade, 29-30 October 2015).

4.3 ASEAN Regional Forum

The ASEAN Regional Forum (ARF) is one of the main forums for the discussion of CBMs in Asia.[49] In 1995, ARF presented a Concept Paper which envisaged three stages of security cooperation: confidence-building, preventive diplomacy, and conflict resolution.[50] The proposed measures focused on two main areas: a set of principles to ensure a common understanding and approach to interstate relations in the region (i.e. dialogues on security perceptions, publication of white papers); and adoption of comprehensive approaches to security. In 2012, the Ministers of Foreign Affairs adopted the Statement on Cooperation in Ensuring Cyber Security that tasked ARF to promote dialogue on confidence-building, stability, and risk reduction measures among its members.[51] In the Chairman's Statement of the 21st ARF Ministerial Meeting in 2014, ARF was mandated to develop a work plan on ICT security focusing on practical cooperation on CBMs. In support of the process, ARF organised a series of seminars on CBMs in cyberspace and other events focusing on broader issues, including cyber incident response.[52] The ultimate goal of these initiatives was to bring together various communities dealing with technology, security or Internet infrastructure.

The purpose of the Work Plan presented at the Ministerial Meeting in May 2015 is 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'.[53] The objectives included 'promoting transparency and developing confidence-building measures to enhance the understanding of ARF Participating Countries in the ICT environment with a view to reducing the risk of misperception, miscalculation and escalation of tension leading to conflict'.[54] It proposes establishing an open ended Study Group on Confidence Building Measures to submit consensus reports recommending CBMs to reduce the risk of conflict stemming from the use of ICT. It also suggests that reports should draw on previous ARF discussions and relevant work in other regional and international forums. Looking at the proposals of concrete workshops to be organised in support of the Study Group, it is difficult to avoid the impression that they clearly build on

49 ARF brings together 27 states, including ten members of the ASEAN, ten ASEAN dialogue partners (EU, China, US, Russia, Japan, Australia, Canada, New Zealand, India, and South Korea), and DPRK, Mongolia, Pakistan, Timor-Leste, Bangladesh, Sri Lanka and Papua New Guinea (observer).

50 Amitav Acharya, *The ASEAN Regional Forum: Confidence-Building: Draft Report*, PWGSC Contact 041.08011-6-1610/01-SS (1997), http://www.amitavacharya.com/sites/default/files/ASEAN%20Regional%20Forum-Confidence%20Building.pdf.

51 'Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security' (ASEAN Regional Forum, 19th ARF, 2012), http://www.mofa.go.jp/files/000016403.pdf.

52 The workshops and seminars focused on: 'ARF Seminar on Confidence-Building Measures in Cyberspace' (Seoul, 11-12 September 2012), 'ARF Workshop on Cyber Confidence Building Measures' (Kuala Lumpur, 25-26 March 2014), 'ARF Workshop on Space Security' (Hoi An, 6-7 December 2012), 'ARF Workshop on Cyber Incident Response' (Singapore, 6-7 September 2012), 'ARF Workshop on Measures to Enhance Cyber Security – Legal and Cultural Aspects' (Beijing, 11-12 September 2013) and 'ARF Workshop on Cyber Security Capacity Building' (Beijing, 29-30 July 2015): See Asean Regional Forum, 'List of ARF Track I Activities (By Inter-Sessional Year from 1994 to 2015),' http://aseanregionalforum.asean.org/library/arf-activities.html?id=582.

53 'ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies' (ASEAN Regional Forum, 7 May 2015), http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf.

54 Ibid.

Table 3. Summary of UN GGE and OSCE CBMs.[55]

UN GGE 2013 Report and UN GGE 2015 Report recommendations	OSCE Decision 1106
Communication and information exchange	
· 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; · 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, analyse 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; · Exchanges of information and communication between national CERTs bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels; · States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders, through: - Creating a repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of relevant related materials deemed appropriate for distribution; - Development of mechanisms and processes for consultations; - Development of technical, legal and diplomatic mechanisms to address ICT-related requests; - National arrangements to classify ICT incidents in terms of the scale and seriousness.	· Provide national views on various aspects of national and transnational threats to and in the use of ICTs. Facilitate co-operation among the competent national bodies and exchange of information; · 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 establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level; · 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; · 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; explore further developing the OSCE role in this regard; · Nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs; Update contact information annually and notify changes no later than thirty days after a change has occurred; · 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.

55 Author's compliation on the basis of 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures,' PC.DEC/1106; United Nations, General Assembly, Group of Governmental Experts A/68/98; United Nations, General Assembly, Group of Governmental Experts, A/70/174.

Transparency and verification	
· Identification of points of contact at the policy and technical levels to address serious ICT incidents and creation of a directory of such contacts; · Development of and support for mechanisms and processes for consultations to reduce risks of misperception, escalation and conflict; · Encouraging transparency by sharing national views and information on 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; CBMs developed in regional and multilateral forums; and relevant national organisations, strategies, policies and programmes; and · Provision of national views of categories of infrastructure considered as critical and national efforts to protect them, including national laws and policies for the protection of data and ICT-enabled infrastructure.	· Hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict, and to protect critical national and international ICT infrastructures including their integrity; · Share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet; · 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; and · 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. In the longer term, participating States will endeavour to produce a consensus glossary.
Cooperative measures of non-military nature	
· Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile state actions; · Cooperative 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; · Cooperation, including the development of focal points for the exchange of information on malicious ICT use and assistance in investigations; · Creation of a national CERT/CSIRT or officially designating an organisation to fulfill this role. States should support and facilitate the functioning of and cooperation among such national response teams and other authorised bodies; · Expansion and support for practices in CERT/CSIRT cooperation, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organising exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation; and · Cooperation, 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.	· Put in place – if they so decide – 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, in order to counter terrorist or criminal use of ICTs.

the OSCE set of CBMs. The workshops are supposed to explore the feasibility and possible modalities for:

- Voluntary sharing of information on national laws, policies, best practices and strategies as well as rules and regulations on security of and the procedures for information sharing;
- Table-top exercises on preventing ICT-related incidents that may evolve into regional security problems;
- Development of rules, norms, and principles of responsible behaviour and the role of cultural diversity in the use of ICTs;
- Measures to promote cooperation against criminal and terrorist use of ICTs including, cooperation between law enforcement agencies and legal practitioners, possible joint task force between countries, crime prevention and information sharing on possible regional cooperation mechanism;
- Terminology related to ICT security to promote understanding of different national practices and usage;
- Establishment of senior policy points of contact to facilitate real time communication about events and incidents of potential regional security significance; and
- Establishment of channels for online information sharing on threats in ICT, global ICT incidents, and sources of ICT attacks threatening critical infrastructure, and development of modalities for real time information sharing.

Even though these are not framed as CBMs in the strictest sense, they bare clear resemblance to measures developed by the OSCE. Also, since finding compromises within ARF has become complicated given its expanding membership, including actors like the EU, US, China and Russia, it is not surprising that without a strong tradition of multilateral cooperation in the region, the ARF members have opted to first explore the feasibility of certain options. While reaching consensus on concrete measures is difficult due to the complicated relations between some members, different political systems, and levels of development, the intermediate results of the OSCE process might be particularly helpful in identifying measures on which states are most likely to cooperate.

4.4 Organization of American States

The Organization of American States (OAS) launched its efforts to develop CBMs at the First Summit of the Americas in 1994. The Plan of Action adopted at the summit expressed support for actions that encourage regional dialogue and strengthen mutual confidence.[56] OAS also held two regional conferences on confidence- and

56 'Summit of the Americas Plan of Action' (Organization of American States, First Summit of the Americas, Miami, Florida, 9-11 December 1994), http://www.summit-americas.org/miamiplan.htm.

security-building measures in Santiago[57] (1995) and San Salvador[58] (1998) resulting in development of two comprehensive sets of CBMs, including adoption of agreements regarding advance notice of military exercises and exchange of information on defence policies and doctrines.

With an increasing need to address security challenges that could undermine developmental gains stemming from the use of ICTs, the 2002 meeting of the Committee on Hemispheric Security of the Permanent Council addressed the security of critical information systems and considered the need to develop a cyber security strategy. In 2004, OAS adopted the Comprehensive Inter-American Cybersecurity Strategy with an overall aim to foster 'a culture of cyber security that deters misuse of the Internet and related information systems' and encourage 'the development of trustworthy and reliable information networks'.[59] The strategy encompasses a number of initiatives aimed at strengthening trust and confidence in cyberspace, including:

- Formation of an inter-American alert, watch, and warning network to rapidly disseminate cyber security information and respond to crises and incidents;
- Addressing trust issues as an essential element of the hemispheric network in order to create the right environment for CSIRTs to exchange proprietary or otherwise sensitive information. This could be achieved through developing a secure infrastructure for managing sensitive information, enhancing the ability to communicate securely with stakeholders, and establishing procedures to guard against inappropriate disclosure of information;
- Identification and adoption of technical standards for a secure Internet architecture; and
- Building up legal capacities of OAS member states to protect Internet users and information networks. Concrete measures mentioned in the strategy include drafting and enacting effective cyber crime legislation and improving international handling of cyber crime matters.[60]

57 'Declaration of Santiago on Confidence- and Security-Building Measures' (Organization of American States, Regional Conference on Confidence- and Security-Building Measures, Santiago, 8-10 November 1995).

58 'Declaration of San Salvador on Confidence- and Security-Building Measures' (Organization of American States, Regional Conference on Confidence- and Security-Building Measures, San Salvador, El Salvador, 25-27 February 1998), http://www.oas.org/csh/english/csbmdeclarsansal.asp.

59 'Adoption of A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity' (Organization of American States, Fourth Plenary Session, 8 June 2004), http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm.

60 'Adoption of A Comprehensive Inter-American Cybersecurity Strategy'.

The OAS experience is noteworthy since it has taken a different approach to other regions by resorting directly to the development of cooperative measures. For instance, OAS members have made concrete commitments to step up cyber crime and infrastructure protection cooperation. Since the adoption of the strategy, cooperation between responsible national authorities such as Computer Emergency Response Teams and law enforcement agencies has improved consistently with regard to information sharing and technical cooperation. At the same time, the region exhibits imbalances with regard to cyber-related development; while some countries have advanced their technical and investigative capabilities and have in place requisite laws, others still grapple with meeting basic needs such as setting up a CERT or passing cyber crime legislation.[61]

5. Trends in Development of CBMs

As the overview of existing confidence-building initiatives suggests, there is no 'one-size fits all' approach. This stems from different historical and political contexts within which regional organisations operate and differences in their respective powers and decision making procedures. It is therefore important to highlight that the starting point is not the same for everyone: whereas the OSCE was able to draw from its decades-long experience with CBMs, the ASEAN Regional Forum approach is pragmatic and action oriented, including organising seminars and workshops in order to explore the possibility of establishing similar measures in the future.

Despite those differences, it is possible to identify two major trends in the debate about the future development of CBMs. A first trend – broadening the scope of CBMs – describes an increasing focus on building states' cyber capacities to ensure that all countries meet certain baseline levels of capacities that would enable them to participate in the development and implementation of CBMs. That also implies bringing in new actors, including the private sector, utility managers, and academic institutions. A second trend – deepening of CBMs – addresses the proliferation of bilateral cyber pacts between states in order to supplement norms and CBMs developed regionally and internationally with more politically binding arrangements. These quasi-agreements are viewed as a way to provide additional guarantees that their signatories will behave responsibly in cyberspace.

5.1 Broadening Cooperation Through Capacity-Building

The discussion about norms of behaviour and CBMs assumes that states possess a certain level of capabilities that allows them to participate in the implementation of concrete CBMs. For instance, a state which does not have a cyber security strategy

61 Symantec, Organization of American States, *Latin America+Caribbean Cyber Security Trends Report* (June 2014), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OAS-Symantec_Cyber_Security_Report_2014.pdf.

or a functioning CERT will not be able to exchange information about structures in place or contribute to management of specific incident. In that respect, the lack of participation may in some instances be interpreted as hostility. The UN GGE 2015 report explicitly acknowledged the link between compliance with norms and capacity of developing countries. While recognising that decision makers, in particular politicians, military staff and diplomats, are the primary addressees of the CBMs, one cannot ignore the fact that in order to take informed decisions, they need to rely on and interact with technical experts, law enforcement agencies and the private sector.

The scope of the existing challenges and the variety of financial and human resources needed to address them, require framing development of CBMs as a multi-level and multi-stakeholder engagement involving all parts of government and the private sector. Given that protection of ICT-enabled infrastructure and adequate response capacities in case of attacks is evolving into one of the main norms of behaviour in cyberspace, cooperation models among the incident respondents' community emerges as one of the key confidence-building elements. Various models of cooperation are already in place and could be increasingly involved in CBMs, ranging from assistance in establishing national CERTs[62] to bilateral team-to-team cooperation.[63] For instance, FIRST is a global 'trust network' composed of more than 300 computer security incident response teams from the public and private sectors.[64] FIRST strengthens trust within the global incident response community by fostering coordination in incident prevention and response, as well as by promoting information sharing among members. Similar venues have been established at the regional level, including AP-CERT[65] for Asia Pacific and AfricaCERT[66] for improving cooperation among African countries.

Certain steps were also made towards building and strengthening law enforcement and judicial capacities of countries in need of assistance, including through developing adequate legal frameworks, training of law enforcement officials, and strengthening cyber forensic capacities.[67] With regard to law enforcement cooperation, UN General Assembly Resolution 55/63 of 2001 calls on states to prevent their territories from being used as safe havens and to cooperate in the investigation and prosecution of international cyber attacks.[68] Similarly, the efforts undertaken in the framework of the Council of Europe Convention on Cybercrime – the only international legally binding treaty on the fight against cyber crime – are worth mentioning.[69]

62 Deloitte Bedrijfsrevisoren and Lionel Ferette, European Union Agency for Network and Information Security, 'Supporting the CERT Community "Impact Assessment and Roadmap"', Ver. 1.0 (1 December 2014), https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap.

63 European Union Agency for Network and Information Security, 'CERT Cooperation and Its Further Facilitation by Relevant Stakeholders,' Deliverable WP 2006/5.1(CERT-D3) (2006), http://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders.

64 FIRST, www.first.org.

65 APCERT, www.apcert.org.

66 AfricaCERT, www.africacert.org

67 European Union, Council of Europe, *Capacity Building on Cybercrime*: *Discussion Paper* (1 November 2013), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6.

68 United Nations, General Assembly resolution 55/63, *Combating the Criminal Misuse of Information Technologies*, A/RES/55/63 (22 January 2001), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

69 Council of Europe, *Convention on Cybercrime: CETS No. 185* (Budapest, 2001), http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

Some countries and international actors have also established bilateral venues for cooperation. The EU, for instance, has established a number of dialogues with third countries to enhance cooperation in the fight against cyber crime.[70] In September 2015, the US and China agreed to establish a 'high-level joint dialogue mechanism on fighting cyber crime and related issues'. The dialogue will focus on concrete confidence-building measures such as review of the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side; establishing a hotline for the escalation of issues that may arise in the course of responding to such requests. Both sides also agreed to cooperate with requests to investigate cyber crimes and provide updates on the status and results of those investigations, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.

5.2 Deepening Cooperation Through Bilateral Agreements

In recent years, states have also increasingly opted for entering into bilateral agreements – either as formal international treaties or more informal political arrangements – in cases where the limited trust needed to be compensated with additional verification and enforcement mechanisms. The examples of such agreements include:

- *US-Russia agreement.* In June 2013, the US and Russia signed a landmark agreement to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern.[71] The US-Russia pact foresees the establishment of a hotline as one of the components in the existing Direct Secure Communication System between the White House and the Kremlin, and the exchange of technical information between the US Computer Emergency Response Team and its Russian counterpart. To avoid any risk of misperception and escalation, both sides agreed to expand the role of the Nuclear Risk Reduction Centre established in 1987 to exchange information about planned cyber exercises or cyber incidents.
- *Russia-China agreement.* In May 2015, Russia and China concluded a non-aggression agreement by virtue of which both sides agreed to refrain from cyber attacks against each other and to jointly respond to technologies that may have a destabilising effect on political and socio-economic life or interfere with the internal affairs of the state.[72]

70 Patryk Pawlak, *Cyber diplomacy: EU Dialogue with Third Countries: Briefing* (European Parliamentary Research Service, June 2015), http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI%282015%29564374_EN.pdf.

71 The White House, Office of the Press Secretary, *Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security*, 17 June 2013, https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

72 See Olga Razumovskaya, 'Russia and China Pledge Not to Hack Each Other,' *Wall Street Journal*, May 8, 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/; Andrew Roth, 'Russia and China Sign Cooperation Pacts,' *New York Times*, May 8, 2015, http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html.

- *US-China agreement*.[73] Announced during President Xi Jinping's visit to Washington in September 2015, this agreement expresses in clear terms the both parties' commitment to the some of the peace-time norms outlined in the 2015 UN GGE report. Both sides have agreed to a number of CBMs, including to provide one another with a timely response to requests for information and assistance concerning malicious cyber activities, and to refrain from conducting or knowingly-supporting cyber-enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors.[74] Speaking of the 'consensus' reached between China and the US, Foreign Ministry spokesperson Hong Lei said that it 'will help enhance mutual trust and promote cooperation between the two countries in this regard, and have positive effects on the sound and steady growth of China-US relations.'[75]

Since public knowledge about the content of these agreements is limited to information provided in press releases and official statements, it is hard to assess their impact on the development of CBMs. It is fair to assume, however, that since most disagreements exist on Washington-Moscow-Beijing axis, any agreements reached between the representatives of these countries are likely to shape the future development of confidence-building measures. At the same time, the lack of transparency surrounding these agreements, while supposedly improving the relations between their signatories, may create suspicion and diminish confidence of those not directly involved.

6. Stability in Cyberspace: What Future Role for CBMs?

The analysis presented in this chapter confirms the importance which international and regional organisations attach to the development of CBMs. This is not surprising given the potential negative impact that misunderstanding and miscalculation in cyberspace might have on international stability. Development of CBMs has been so far closely associated with the process of establishing norms of behaviour in cyberspace as a means to reduce the risk of misunderstandings but also indirectly to ensuring a continuous monitoring of the commitments to which individual states have subscribed. This is achieved through specific measures focused on increasing

73 Two more general Memoranda of Understanding on Confidence Building Measures (CBMs) in the field of military relations were signed between China and the US in November 2014. The White House, Office of the Press Secretary, *Fact Sheet: President Xi Jinping's State Visit to the United States*, 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

74 Ibid.

75 Ministry of Foreign Affairs of the People's Republic of China, *Foreign Ministry Spokesperson Hong Lei's Regular Press Conference*, 28 September 2015, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1301373.shtml.

transparency and communication. At the same time, there is a growing realisation in policy circles that compliance with the commitments is linked to the question of capacities of individual states.

As the result, norms, CBMs and capacity-building emerge as three main pillars in the process of developing a sustainable and stable digital environment. Analysing the linkages between the three, it is possible to distinguish two distinct models for the role of CBMs within this process: a demand-driven model, whereby CBMs play a complementary role in the operationalisation of norms; and a supply-driven model whereby CBMs emerge as a consequence of cyber capacity development.

In the *demand-driven model* for secure and stable cyberspace (Figure 1) norms of behaviour in cyberspace (both non-binding and encompassed in the international law) provide the impulse for development of CBMs. As shown in Table 2, in order to ensure effective implementation of certain norms it is necessary to develop CBMs. At the same time, the scope of CBMs may require engaging in capacity-building activities as a way to ensure that certain benchmarks of human, institutional, technological or legal capacity are achieved, and allows a given state to actively participate in the implementation of the CBMs. That also implies that, with the progressing development of capabilities, there might be a need to redefine or agree supplementary norms. Realisation of this possibility is essential in order to ensure that decisions about capacity development contribute to more trusted and stable cyberspace rather than a potential cyber arms race. The OSCE approach, at least at this stage, seems to be following this logic.

In the *supply-driven model*, the impulse for development of CBMs is provided by progressing development of cyber capacities. This model is not very much present in the ongoing debates. This is understandable given that the discussion about norms is primarily the matter of state relations whereas cyber capacities are generated primarily by non-state actors (including the private sector, cyber criminals, and hackers). In the supply-driven model, CBMs are developed primarily to minimise the risks to delivery of services or products with the use of ICTs. This implies developing concrete cooperative CBMs between all stakeholders, including law enforcement agencies or technical communities. Norms are then developed with the primary objective to regulate the states use of the existing and future capabilities. To some degree, this model was much more dominant in the 1990s when the discussion about the peaceful use of ICT was initiated. It then evolved towards a more demand driven model. The OAS approach to developing confidence-building measures is probably the closest to this model in that it uses the capacity-building processes such as the support provided for setting up CERTs, cyber crime legislation, and cyber security strategies to almost simultaneously promote the development of CBMs including points of contact and CERT-to-CERT cooperation. The ARF approach is guided by a similar logic and driven by the analysis of the existing capacities that could provide the foundation for development of concrete CBMs. Another approach – not discussed at length in this chapter but nonetheless

worth mentioning – adopted in the framework of the Wassenaar Arrangements[76] in December 2013 foresees restrictions on exports of IP network surveillance systems and intrusion software[77] in order to prevent 'cyber proliferation'.[78] The restrictions were imposed, among others, on 'zero-day' exploits which are purchased by governments for the purpose of targeted attacks.[79]

Figure 1. Demand-driven model.

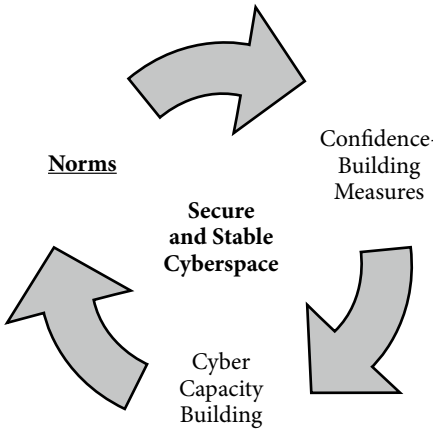
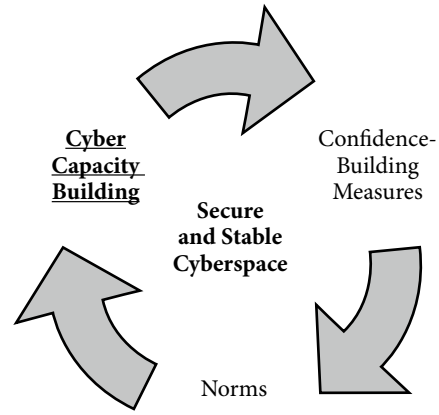


Figure 2. Supply-driven model.



These models, although definitely requiring further elaboration, allow drawing two main conclusions with regard to the future development of CBMs. First, understanding the underlying dynamic relationship between norms, CBMs, and capacity-building within the existing models is essential for building bridges between various regional approaches beyond those discussed in this chapter. For instance, the International Code of Conduct for Information Security promoted by the Shanghai Cooperation Organization recognises the need to develop CBMs aimed at increasing predictability and reducing the likelihood of misunderstanding and the risk of conflict. This includes the voluntary exchange of information regarding national strategies and organisational structures, the publication of white papers

76 It is an international regime regulating exports of conventional weapons and sensitive dual-use items and technologies with military end uses. The participating states of the Wassenaar Arrangements are: all EU member states (except for Cyprus), Argentina, Australia, Canada, Japan, Mexico, New Zealand, Norway, South Korea, Russia, South Africa, Switzerland, Turkey, Ukraine, and US. See 'The Wassenaar Arrangement,' www.wassenaar.org.

77 Jennifer Granick, *Changes to Export Control Arrangement Apply to Computer Exploits and More* (Stanford Law School, The Center for Internet and Society, 2014), http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more.

78 Sam Jones, 'Cyber War Technology to be Controlled in Same Way as Arms,' *Financial Times*, December 4, 2013, http://www.ft.com/intl/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html#axzz3wSJjk22o.

79 Brian Fung, 'The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities,' *Washington Post*, August 31, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/.

and exchanges of best practice.[80] With the official aim to create more reliable and cooperative environment between its signatories, the Code had the opposite impact on relations with other members of the international community – notably European Union and the US – who expressed concern that some of the provisions in the document can be interpreted in a way that is not compatible with existing international law, and in particular human rights law. In a similar vein, the Communique issued in October 2015 by the BRICS countries highlights the need 'to promote measures and facilitate favourable conditions for ensuring the progressive development of ICTs … such as the equitable use of security measures relating to the continuity and stability of the use of ICTs in all spheres of life and production'.[81]

Second, it is crucial to understand the role of capacity-building in the development of CBMs and ensuring the stability of cyberspace in general. It is not to say that the process of capacity-building automatically leads to more unstable and unpredictable cyberspace. As a matter of fact, capacity-building projects implemented nowadays focus on using ICT to stimulate social development, human security and economic growth. Ironically, bringing the elements of capacity-building into the discussion about CBMs might also offer a solution to one of the main weakness of the existing CBMs; their voluntary nature and the absence of compliance verification mechanisms. By engaging with product designers or utility managers from the very beginning it might be possible to prevent certain undesired developments and enhance cooperation between those actors without a need for additional CBMs. This point is particularly important in light of the growing use of ICT platforms and a potential inability to continuously expand CBMs to those new policy areas.

7. Conclusion

The development of confidence-building measures is closely linked to the debate about norms in cyberspace. However, the examples from different regional organisations currently engaged in developing CBMs show that while norms help to establish certain benchmarks for responsible state behaviour, the difficulties with attributing certain acts and still nascent opportunities for verification call for defining alternative solutions that could help overcome limited trust and reduce the risks of misunderstandings. CBMs have emerged as one such alternative. Consequently, the chapter has focused on confidence-building processes within the UN

80 United Nations, General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/69/723 (13 January 2015), https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

81 'Communique of BRICS Ministers of Communications on the Outcomes of the Meeting on "Expansion of Cooperation in the Field of Communications and ICTs"' (Meeting of ICT Ministers of the BRICS group, Moscow, 23 October 2015), https://en.brics2015.ru/load/637860.

framework and at the regional level, including in the OSCE, OAS and ARF. A closer analysis of these processes points to the emergence of two overarching trends: an increasing significance of the capacity-building processes in order to help individual states meet their commitments, and assuring additional guarantees through bilateral agreements. This has led to the conclusion that norms, CBMs and capacity-building constitute three pillars on which stability in cyberspace needs to be constructed. Finally, looking at the drivers for development of CBMs, the chapter suggests that the ongoing efforts can be better understood through demand-driven and supply-driven models.