In: IFSH (ed.), OSCE Yearbook 2017, Baden-Baden 2018, pp. 201-212.

Velimir Radicevic

Promoting Cyber Stability between States: OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs) in the Context of Global and Regional Security

Introduction – The Global Status Quo in Cyberspace

As a borderless resource employed in almost every sector and state, the internet has enhanced the prospects for economic growth, political discourse, information dissemination, and social mobility around the globe, ushering in what some are calling the third industrial revolution. However, the rapid promulgation of this resource went hand in hand with the rise of new challenges – malware, hacking attacks, data breaches, and cyber espionage, just to name a few – from as early as 1988, when the "Morris worm" facilitated the first documented Distributed Denial-of-Service (DDoS)[1] attack. Since then, due to the unique combination of high profitability and impact, low technological barriers to entry, and asymmetrical risks to the perpetrators, the breadth and scope of cyber-attacks have continued to grow. This was seen in recent high-profile cyber incidents, such as the WannaCry ransomware attack, efforts to hack elections in the US and France, and attacks against critical infrastructure in Ukraine and Georgia. The difference between such wide-ranging attacks and everyday cybercrime and terrorist uses of the internet may seem academic, but the scope and sophistication of such attacks led many experts to believe they could only have taken place with some form of state involvement.

In addition, states have recognized the advantages of cyber-attacks and have correspondingly begun to enhance their defensive and offensive cyber capabilities. According to the United Nations Institute for Disarmament Research (UNIDIR), over 47 States have cyber/ICT security programmes that give some role to the armed forces,[2] and some have defined cyberspace itself

Note: The views expressed in this article are those of the author and do not necessarily reflect the official position of the OSCE. The author would like to thank Veronika Černá, project assistant on cyber/ICT security in the Co-ordination Cell, Transnational Threats Department of the OSCE Secretariat, for her valuable assistance.

1 A DDoS attack is a cyber-attack in which one party seeks to make a single computer, or a computer network, unavailable to its intended users, usually by flooding the targeted machine(s) with superfluous requests in an attempt to overload systems and prevent legitimate requests from being fulfilled.

2 Cf. James Andrew Lewis, Cybersecurity and Cyberwarfare: Assessment of National Doctrine and Organization, United Nations Institute for Disarmament Research (UNIDIR),

as a domain of potential military operations.[3] This digital arms race, paired with the borderless nature of cyberspace, the difficulties of assigning responsibility for cyber-attacks (attack attribution), and the differences in cyber capabilities among states, have added confusion, uncertainty, and misperception to inter-state relations. This, in turn, can lead to escalating tensions between states and can potentially morph into kinetic conflict.

Unfortunately, there are few established methods to alleviate this confusion and reduce potential tensions stemming from the use of ICTs. It is not likely that there will be a cyber equivalent to the Treaty on Open Skies[4] in the near future – or ever – capable of building confidence through a multilateral regime of arms control in cyberspace. Cyber tools are not visible or easy to itemize, and servers can be rented or used by criminal groups to launch attacks from across the globe to further avoid detection. And when an attack does happen, its attribution, even when accurate and timely, can fail to establish a clear link between the perpetrator and a potential state actor suspected of being behind it.[5]

All of this means that cyber/ICT security has quickly grown in prominence on the agendas of states and, subsequently, international, regional, and sub-regional organizations, all of which face the same question: What is needed to enhance global cyber stability between states and reduce tensions that can grow from an ICT-enabled incident?

International Law, Potential Applications in Cyberspace, Norms of State Behaviour, and Confidence-Building Measures

Individual states have the ability to regulate access and usage of the internet through national legal frameworks. However, cyberspace is still significantly younger than the mechanisms that form the core of international law, such as the UN Charter, the Geneva Convention, the Helsinki Final Act, and the International Covenant on Civil and Political Rights (ICCPR). Without treaty or customary law to inform rules and norms of responsible state behaviour in cyberspace, and with no courts to give rulings based on them, the central question becomes one of the applicability of existing international laws in cyberspace – in particular regarding *jus ad bellum* and *jus in bello*. Can they be applied? If they can, how and under what circumstances? What is the threshold that qualifies a cyber incident as an attack that can trigger Article 51 of

---

The Cyber Index. International Security Trends and Realities, New York/Geneva 2013, pp. 9-90, here: p. 14.

3 Cf. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit*, 21 July 2016.

4 Cf. *Treaty on Open Skies*, 1992, available at: http://www.osce.org/library/14127.

5 Cf. Michael N. Schmitt/Liis Vihul, *The Nature of International Law Cyber Norms*, in: Anna-Maria Osula/Henry Rõigas (eds.), International Cyber Norms: Legal, Policy & Industry Perspectives, Tallinn 2016, pp. 23-47, here: p. 38.

the UN Charter? At the level of the United Nations, the question of applicability was answered in 2013 by means of a consensus report recommending the application of existing international laws in cyberspace, thus opening the debate on how exactly to transcribe 20th-century legal codes to this 21st-century legal challenge. Centres like the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have weighed in on the issue, publishing compiled opinions by legal practitioners and scholars on the application of various provisions of international law in the Tallinn Manual on the International Law Applicable to Cyber Warfare[6] and the Tallinn Manual 2.0.[7]

In parallel to discussions on the legal aspects that govern cyberspace, another focus has been on developing non-binding mechanisms that can shape states' expectations about what is acceptable behaviour in cyberspace. These take the form of norms of responsible state behaviour and ways of ensuring that such behaviour is actively exercised through confidence-building measures (CBMs). Norms of responsible state behaviour seek to define key concepts, such as "red lines" for the use of ICTs by states. One example would be that a state should not knowingly allow its territory to be used to launch cyber-attacks against another country, or to knowingly or unknowingly target another state's critical infrastructures or their ICT-enabled control systems. The idea is that such "soft law" can produce certain legal effects by shaping common expectations about a state's conduct in the international sphere,[8] thereby forming the bedrock of customary law for cyberspace. An example of setting such norms of state behaviour in cyberspace can be seen in the International code of conduct for information security proposed by the Shanghai Cooperation Organisation (SCO) in 2011, with an updated version published in 2015.[9]

However, agreeing on norms of responsible state behaviour in cyberspace is not a guarantee of their application, especially given the prevailing risks of misunderstanding and confusion in inter-state relations when the use of ICTs is involved. Practical and actionable measures are needed to operationalize norms in a way that can consistently enhance co-operation and build trust between states. Luckily, a model for these measures already existed in the form of the OSCE Vienna Document on Negotiations on Confidence- and Security-Building Measures (CSBMs) from 1990, which set out voluntary military measures critical for enhancing transparency, trust building, and arms control in the OSCE area. Once adapted for cyberspace,

6 Cf. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York 2013.

7 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Factsheet, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2 February 2017.

8 Cf. Katharina Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, Tallinn 2013, p. 32.

9 Cf. United Nations General Assembly Document A/69/723, *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*, 13 January 2015.

such measures eschewed the military aspects of traditional CSBMs in favour of enhancing cyber diplomacy between states and helping bring both like-minded and non-likeminded states to the table. As such, cyber/ICT security CBMs are recognized as a crucial tool for policy makers on all levels – from the United Nations to regional organizations and national governments.

The discourses on legal provisions, norms of responsible state behaviour, and confidence-building measures, whether ranked or considered as equally important mechanisms, are linked and mutually reinforcing in most high-level efforts to enhance cyber stability between states.

The United Nations Group of Governmental Experts – How It Has Affected Global Discourse Related to Promoting Cyber Stability between States

The lack of clarity on how uses of ICTs in inter-state relations can be normatively defined is compounded by differences in national approaches to cyber/ICT security, divergent terminology and definitions, and differences in culture and priorities. Thus, when the United Nations tackled cyber/ICT security in Resolution A/RES/53/70 on 4 January 1999, it faced a daunting challenge. Significant progress was made in 2003, when the Russian Federation first proposed the establishment of a dedicated group to address cyber/ICT security issues. This group was subsequently formed by A/RES/58/32 on 18 December 2003. The newly formed Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security was made up of states selected on the basis of equitable geographical distribution, along with the five permanent members of the Security Council. The UN GGEs have the goal of producing consensus reports detailing how identified cyber/ICT security threats can best be approached by the international community.

The first GGE report was distributed as General Assembly (GA) Document A/65/201 on 30 July 2010. The report provided a broad overview of cyber/ICT security threats faced by states and the types of co-operative measures that can be undertaken to mitigate them. Its recommendations included a blueprint for successive UN GGEs to tackle the issue, with a focus on international norms pertaining to state uses of ICTs and confidence-building measures to "reduce the risks of misperceptions resulting from ICT disruptions".[10] There was no discussion of international law in the 2010 report, but this topic would assume a prominent place in the 2013 report, published as A/68/98.[11] As part of its section on norms, rules, and principles of

10 Cf. United Nations General Assembly Document A/65/201, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 July 2010.

11 Cf. United Nations General Assembly Document A/68/98, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 24 June 2013.

the responsible behaviour of states, the report cited international law and the UN Charter in particular, as well as the norms, rules, and principles derived from it, as being essential to maintaining an open and secure ICT environment. The report also stated that "states must meet their international obligations regarding internationally wrongful acts attributable to them".[12] While not going more in-depth than this on the application of international law to cyberspace, this report would serve as a powerful framework for future discussions on the topic. Regarding CBMs as the third component of cyber stability, the report stated 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".[13]

The report also highlighted the role of regional organizations, such as the OSCE, the Association of Southeast Asian Nations Regional Forum (ARF), and the Organization of American States (OAS), in promoting cyber stability and resilience among their members. This reference was deliberate. Regional organizations can use their accumulated political capital and their pre-established institutional capacities to bring together non-likeminded states to address common security challenges such as enhancing cyber stability. As will be discussed below, the OSCE has led the way in this field since 2012 and has been developing confidence-building measures through the Informal Working Group (IWG) established pursuant to Permanent Council (PC) Decision No. 1039.[14] The OSCE and the UN have continued to affect each other's work, with the UN GGE reports framing cyber/ICT security discussions in the OSCE and the OSCE's experience with confidence-building measures informing future UN GGE reports.

The 2015 UN GGE Report, published as UN General Assembly Document A/70/174,[15] elaborated on international laws, norms of responsible state behaviour, confidence-building measures, and international co-operation and assistance in capacity-building as equal and critical pillars of global cyber stability. The group recommended its own general CBMs for the consideration of member states, which aimed at increasing transparency, facilitating consultations and co-operation, reducing the risk of misperception, escalation, and conflict and protecting critical infrastructure. It also continued to support "regular dialogue through […] regional and multilateral forums",

12 Ibid., p. 2.
13 Ibid., p. 9.
14 Cf. Organization for Security and Co-operation in Europe, Permanent Council, *Decision No. 1039, Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1039, 26 April 2012, available at: http://www.osce.org/pc/90169.
15 Cf. United Nations General Assembly Document A/70/174, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, at: http://undocs.org/A/70/174.

while acknowledging "the valuable efforts in ICT security made by international organizations and regional groups" such as the OSCE.[16]

In spite of its position as the highest-placed multilateral body dealing with topics related to cyber/ICT security and stability, as of 2017 the future of the UN GGE is unclear. The 25-member group has not succeeded in reaching agreement among its members to produce a new consensus report further elaborating on the recommendations of the 2015 UN GGE. According to the group's chair, while no consensus report will be produced, there was still agreement between experts on topics such as emerging risks, capacity-building and confidence-building measures, norms, awareness raising among senior decision-makers, conducting exercises, defining protocols for notifications about incidents, warnings when critical infrastructure is attacked, and preventing non-state actors from conducting cyber-attacks.[17]

OSCE Cyber/ICT Security Confidence-Building Measures and Related Decisions

The UN GGE deliberations have framed the debate on cyber/ICT security in an international context, but it is up to other bodies working at the national, sub-regional, and regional levels to facilitate the adoption and implementation of its recommendations. In line with this, the OSCE PC took the decision to "step up individual and collective efforts to address security in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner" in PC Decision No. 1039, adopted on 26 April 2012.[18] This decision established an open-ended, informal OSCE working group tasked with elaborating confidence-building measures to reduce the risks of conflict stemming from the use of ICTs. The work on the CBMs was recognized in Ministerial Council Decision No. 4/12 of 7 December 2012,[19] which listed cyber/ICT security as one of the four key transnational threats and strategic priorities of the OSCE. Also in 2012, the OSCE established the post of Cyber Security Officer (CSO) within its newly created Transnational Threats Department (TNTD), to act as the principal focal point of all cyber/ICT security issues for all 57 participating States, as well as other OSCE executive structures.

Following a series of ad hoc meetings, the PC adopted Decision No. 1106 on 3 December 2013 in Vienna, thereby creating the first real set of

16 Ibid., pp. 9-10, 14.
17 Cf. Geneva Internet Platform, *UN GGE: Quo Vadis?* Digital Watch Newsletter, Issue 22, June 2017, pp. 6.
18 Cf. PC.DEC/1039, cited above (Note 14).
19 Cf. OSCE, Organization for Security and Co-operation in Europe, Ministerial Council, Dublin 2012, *Decision No. 4/12, OSCE's Efforts to Address Transnational Threats*, MC.DEC/4/12, 7 December 2012, available at: http://www.osce.org/mc/97959.

OSCE confidence-building measures.[20] These measures sought to reduce the risks of conflict between OSCE participating States stemming from the use of ICTs by encouraging timely consultations; using the OSCE as a platform for dialogue, information, and the exchange of best practices; sharing national views on cyber threats and cyber/ICT security policy papers, policies, and programmes; providing lists of relevant terminology; and forming a network of points of contact to help co-ordinate whole-of-government responses to ICT-related incidents.

In short, the initial set of OSCE CBMs promoted transparency that would allow states to read one another's "posture" in cyberspace, facilitate meaningful communication between them and enhance regional cyber resilience in order to create a stable and secure "cyber neighbourhood" in the OSCE area. Decision No. 1106 also transformed the IWG from an ad hoc arrangement into a series of at least three meetings each year, with participating States continually exchanging information on CBMs through established OSCE platforms, such as the POLIS OnLine Information System.

Over the subsequent two years, discussions were held on how to build on the initial set of CBMs. In 2016, after much debate, five new measures were introduced in PC Decision No. 1202 of 31 March 2016.[21] The key areas of the second set were defined as: practical collaboration on critical infrastructure protection, expansion of the crisis communication channels, and the enhancing of cyber resilience through co-operation with the private sector. This means that the OSCE has entered 2017 with sixteen practical and actionable measures, with support for their implementation coming from Ministerial Council Decisions No. 5/16[22] and No. 5/17.[23]

The underlying qualities of these aspects of the CBMs – their connection to recommendations of UN GGE reports, the level of political support given by participating States, and their potential for practical implementation – make them powerful and unique tools, not just in the OSCE area, but as a source of good practices and lessons for other organizations to replicate.

---

20 Cf. Organization for Security and Co-operation in Europe, Permanent Council, *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, 3 December 2013, available at: http://www.osce.org/pc/109168.

21 Cf. Organization for Security and Co-operation in Europe, Permanent Council, *Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, PC.DEC/1202, 10 March 2016, available at: http://www.osce.org/pc/227281.

22 Cf. Organization for Security and Co-operation in Europe, Ministerial Council, Hamburg 2016, *Decision No. 5/16, OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, MC.DEC/5/16, 9 December 2016, available at: http://www.osce.org/cio/288086.

23 Cf. Organization for Security and Co-operation in Europe, Ministerial Council, Vienna 2017, *Decision No. 5/17, Enhancing OSCE Efforts to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, MC.DEC/5/16, 8 December 2017, available at: https://www.osce.org/chairmanship/361561.

Focus in 2017: Progress towards an OSCE Crisis Consultation Mechanism

For the CBMs to be effective, they need to be fully operationalized. Following Ministerial Council Decision No. 5/16, efforts by the IWG have focused on the operationalization of rapid communication at the technical and policy levels in order to reduce tensions and risks of conflict stemming from the use of ICTs. In the language of the two PC Decisions, this translates to the setting up of a crisis consultation mechanism consisting of CBMs 3, 8, and 13.

When faced with a cyber/ICT security incident, the first few hours are the most important but also the most likely to be dominated by confusion, misunderstandings, and misattribution. The danger stemming from this type of confusion only increases if the incident in question targets resources critical to the normal functioning of a state, and if suspicion falls on another, non-likeminded state or regional rival. In order to prevent an escalation of tensions stemming from such cases, it is crucial that secure lines of communications be established between national points of contact. These can then help the affected state to obtain critical information regarding the attack from its suspected counterpart, to mitigate its consequences, and to jointly manage the public response to the crisis.

The OSCE has guided the creation of a consultation mechanism that would facilitate such responses through CBMs 3, 8, and 13. Respectively, these CBMs encourage states to hold appropriate-level consultations to reduce risks, to form a network of policy and technical-level points of contact to conduct such consultations, and to use a secure communication channel that would facilitate such contact. The three CBMs form a triangle that helps to answer the fundamental questions of "who" triggers "which" mechanism and "how"/"when". Once fully operationalized and deployed, the network will provide OSCE participating States with a unique tool to manage international cyber incidents and their inevitable fallout.

How CBMs Can Be Deployed in an ICT-Enabled Crisis Scenario

It is important to stress that, while CBMs aim to build trust and therefore reduce the risks of unintentional conflict, they cannot prevent a deliberate international cyber-attack launched by one party against another. In those circumstances, what they can provide to all parties is a method to immediately communicate through points of contact and head off the further escalation of tensions. This can extend to the OSCE's mediating a potential dispute involving the use of ICTs between participating States.

The life cycle of the CBM process can best be illustrated through a hypothetical example. Let us suppose that State A is the victim of a massive cyber-attack targeting its critical energy infrastructure and that its technical appointee has evidence of an unusually large amount of outbound traffic

coming from State B. An observer is likely to first assume either that State B has launched a direct cyber-attack or that it employed a third party to accomplish this. At this point, when both states are still analysing the situation, the CBMs could first be employed. If State B has shared sufficient information through OSCE platforms to help form a view of its capabilities and activities, relevant stakeholders from State A could possibly see whether the attack corresponds to State B's posture in cyberspace. If not, then the possibility that the attack was merely routed through State B's territory or launched without State B's direct knowledge would become more likely. In parallel to this, the points of contact of both states could engage using the OSCE Crisis Consultation Mechanism to exchange critical information, request assistance, and plan a joint response to the unfolding crisis.

In this hypothetical situation, states can use a number of key CBMs to help mitigate an ICT-enabled crisis, expose potential misinformation, and cooperate through established OSCE networks to reduce tensions. Given the rising number of high-profile cyber-attacks and incidents in recent times, it is possible that this kind of abstract scenario could play out in the near future, with the full deployment of any and all operationalized CBMs.

Remaining Challenges and Solutions to CBM Implementation

Apart from the Crisis Consultation Mechanism-related CBMs, the nominal implementation rate across all CBMs, as defined by the percentage of participating States implementing at least one of the sixteen measures, stands at a very high rate of 91 per cent. Given that the OSCE cyber/ICT security CBMs are a voluntary mechanism and implementation relies on the recognition of their practical usefulness by participating States, this represents an especially high percentage. However, this implementation rate does not reveal the whole picture. For instance, while most participating States are actively engaged in the process, not all states have found every CBM to be an equal priority – the average implementation rate across all sixteen CBMs is around 40 per cent. Further, simply viewing CBM implementation through percentages fails to illustrate the obstacles states face when implementing individual measures.

This is why it was necessary to first identify the principal implementation challenges, while keeping in mind the unique national and sub-regional circumstances that may help or hinder the operationalization of measures. This task required extensive open source data collection and analysis, as well as a fresh, unbiased perspective, which was why participating States recommended that the OSCE should "consider entrusting academia with conducting comparative analyses of the information shared in the implementation of

the first set of CBMs".[24] In line with this recommendation, and with the backing of Italy, Germany, and Switzerland, the OSCE TNTD launched an initiative together with the Department of Political and Social Sciences at the University of Florence in 2016. This partnership was then expanded through the formation of an informal Academic Steering Group, made up of research and academic bodies from across the OSCE area.

This joint effort bore fruit in 2017 through two papers:

a) A research report titled "Analysis of the Implementation of the Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", and
b) "Academic proposals for a Work Plan to support the implementation of CBMs", which identified and captured specific tools, measures, and mechanisms, including capacity-building activities, to meaningfully enhance CBM implementation.

Going forward, OSCE TNTD will help address the principal challenges to CBM operationalization identified through the academic Work Plan, for example by demystifying CBMs through E-learning modules and developing the capacities of policy-makers through a series of comprehensive, regional, scenario-based discussions.

CBMs beyond the OSCE Area – Other Regional Mechanisms and OSCE Inter-Regional Initiatives on Cyber/ICT Security

Building confidence to reduce tensions and risks of conflict that may arise from the use of ICTs is a truly global task, which means that the loss of confidence in one region of the world due to the malicious use of ICTs can threaten security and stability outside of its boundaries. Conversely, measures that strengthen confidence and promote security and stability in one region can have a stabilizing effect on states in another. Further, as discussed in the section on the work of the UN GGE, regional organizations and mechanisms can serve as optimal vehicles for the implementation and co-ordination of international security recommendations, including the development of cyber/ICT security CBMs. This underlines the necessity of being aware of and actively promoting interlinkages with other regional processes. In the Americas, for instance, the OAS decided to establish a working group on cooperation and confidence-building measures in cyberspace at the meeting of the Inter-American Committee against Terrorism (CICTE) on 10 April

24 OSCE Switzerland 2014, *OSCE Chairmanship Event Summary, Information and Communication Technologies (ICT) Confidence Building Measures (CBMs): Promoting implementation, supporting negotiations*, CIO/GAL/238/14, 22 December 2014, p. 1.

2017,[25] while in the Asia-Pacific region the ARF ministers endorsed a proposal to establish the ARF Inter-Sessional Meeting on cyber/ICT security at the 24th ASEAN Regional Forum on 7 August 2017.[26]

OSCE Partners for Co-operation and Practical Collaboration

The OSCE itself extends beyond the Euro-Atlantic region, having formed two long-standing groups of Asian and Mediterranean Partners for Co-operation, consisting of Afghanistan, Australia, Japan, the Republic of Korea, and Thailand on the one hand and Algeria, Egypt, Israel, Jordan, Morocco, and Tunisia on the other. Over time, the Partners and the 57 OSCE participating States have developed commitments to explore various avenues of co-operation, such as PC Decision No. 571,[27] adopted on 2 December 2003. This decision encouraged the Partners for Co-operation to "voluntarily implement OSCE norms, principles and commitments" and "to explore the scope for [their] wider sharing". In the domain of cyber/ICT security, this translated into joint activities to identify avenues of co-operation, the exchange of good practices and lessons learned, as well as efforts to harmonize parallel CBM processes across regional divides. Since 2016, these activities have included:

- *Conferences with Asian Partners* – The OSCE Asian Conference held in Bangkok on 6-7 June 2016 included a side event on strengthening cyber/ICT security, re-shaping current dynamics in the OSCE area, affirming the roles of regional organizations, and exploring potential avenues of co-operation with Asian Partners. This was explored further at the Inter-regional Conference on Cyber/ICT Security, held in Seoul on 4-5 April 2017.
- *Initiative at the Global Forum for Cyber Excellence (GFCE)* – On 31 May 2017, the OSCE and Germany launched a joint initiative aimed at linking current discussions across regional forums, accelerating the implementation of CBMs, and further exploring the conceptual link between norms of responsible state behaviour in cyberspace and capacity- and confidence-building. This is to be achieved through active partnerships with regional organizations such as the OAS, ARF member states, and the African Union (AU).

25 Cf. Inter-American Committee Against Terrorism (CICTE), *Establishment of a Working Group on Cooperation and Confidence-Building Measures in Cyberspace*, CICTE/RES. 1/17, 10 April 2017.

26 Cf. 24th ASEAN Regional Forum, Chairman's Statement, *Partnering for Change, Engaging the World*, Manila, Philippines, 7 August 2017, p. 7.

27 Cf. Organization for Security and Co-operation in Europe, Permanent Council, *Decision No. 571/Corrected re-issue, Further Dialogue and Co-operation with the Partners for Co-operation and Exploring the Scope for Wider Sharing of OSCE Norms, Principles and Commitments with Others*, PC.DEC/71/Corr.1, 2 December 2003, available at: http://www.osce.org/pc/18297.

Conclusions

With the promulgation of ICTs, the need for a stable, resilient, predictable, and safe cyberspace is only expected to grow. Cyber/ICT security threats, which are quintessentially transnational, will require greater engagement and commitment from the international community if they are to be faced effectively and to prevent the escalation of tensions and associated risks. At the same time, while the danger seems obvious, finding means to address it is less straightforward. It requires interaction among numerous stakeholders with diverse priorities and agendas, as well as answering unresolved questions concerning international law, norms of responsible state behaviour, and measures for building confidence between states. As has been seen with the most recent UN GGE, there are no guarantees of success for even the most comprehensive process addressing this topic.

Within the OSCE, the CBM process is, in many ways, still in its early stages – key measures have yet to be operationalized, implementation challenges need to be addressed, and inter-regional co-operation on cyber/ICT security has to be institutionalized. However, for its part, thanks to the commitment of its participating States and Partners for Co-operation, the OSCE has achieved measurable progress since 2012 through PC Decisions 1039, 1106, and 1202, Ministerial Council Decisions 5/16 and 5/17, and the continued work of the IWG and the OSCE CSO. The OSCE and the TNTD remain committed to the CBM process and the enhancement of cyber stability and resilience in the OSCE area and beyond.