SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Building Confidence in the Cybersphere: A Path to Multilateral Progress

By Theresa Hitchens and Nancy W. Gallagher, PhD

CISSM Working Paper

March 2018

This working paper was made possible by support from the Carnegie Corporation of New York and the Yamamoto-Scheffelin Endowment for Policy Research.

Center for International and Security Studies at Maryland
4113 Van Munching Hall, School of Public Policy
University of Maryland
College Park, MD 20742
(301) 405-7601

Introduction

As use of the Internet has become critical to global economic development and international security, there is near-unanimous agreement on the need for more international cooperation to increase stability and security in cyberspace. Several multilateral initiatives over the last five years have begun to spell out cooperative measures, norms of behavior, and transparency and confidence-building measures (TCBMs) that could help improve mutual cybersecurity.

These efforts have been painstakingly slow, and some have stalled due to competing interests. Nonetheless, a United Nations (UN) Group of Governmental Experts (GGE) and the Organization for Cooperation and Security in Europe (OSCE) have achieved some high-level agreement on principles, norms, and "rules of the road" for national Internet activities and transnational cyber interactions. Their agreements include commitments to share more information, improve national protective capacities, cooperate on incident response, and restrain certain destabilizing state practices.

Voluntary international agreements are worth little, unless states implement their commitments. So far, implementation has been crippled by vague language, national security considerations, complex relations between public and private actors in cyberspace, and privacy concerns. This is particularly true regarding the upfront sharing of information on threats and the willingness of participants to cooperate on incident investigations, including identifying perpetrators.

With multilateral forums struggling to find a way forward with norm-setting and implementation, alternate pathways are needed to protect and build on what has been accomplished so far. Different strategies can help advance implementation of measures in the UN and OSCE agreements. Some commitments, such as establishing and sharing information about national points of contact, are best handled unilaterally or through bilateral or regional inter-governmental cooperation. Other objectives, such as protecting the core architecture and functions of the Internet that support trans-border critical infrastructure and underpin the global financial system, require a multi-stakeholder approach that includes not only governments but also private sector service providers, academic experts, and nongovernmental organizations.

This paper compares what the GGE and OSCE norm-building processes have achieved so far and what disagreements have impeded these efforts. It identifies several priorities for cooperation identified by participants in both forums. It also proposes three practical projects related to these priorities that members of regional or global organizations might be able to work on together despite political tensions and philosophical disputes. The first would help state and non-state actors share information and communicate about various types of cybersecurity threats using a flexible and intuitive effects-based taxonomy to categorize cyber activity. The second would develop a more sophisticated way for state and non-state actors to assess the risks of different types of cyber incidents and the potential benefits of cooperation. The third would identify aspects of the Internet that might be considered the core of a public utility, worthy of special protection in their own right and for their support of trans-border critical infrastructure.

Background

Information and communications technologies (ICTs) have become central to modern civilization over the past 20 years. The global economy—from banking to energy, transportation, and even the health sector—depends on rapid, real-time communications provided via the Internet, as well as massive data storage and processing capabilities. Militaries in most developed countries now rely on long-range Internet connectivity to manage both peacetime and wartime operations. Countless humanitarian, environmental, and other civil society groups make heavy use of ICTs, and many individuals can barely function without their smart phones, computers, and other ICT devices.

As the safety and security of the cybersphere has become more vital, it has also come increasingly under threat from a growing number of increasingly sophisticated state and non-state actors. According to Russian-based cybersecurity firm Kaspersky Lab, more than 300,000 new malware files were discovered *per day* in 2016.[1] The vast majority of these files do not threaten critical functions, although some create nuisance for customers and operators. Yet, the pace of development of malicious code should give concern. Kaspersky's 2016 annual report also found that more malware is now mass-produced (easing the work of criminals) and that the use of crypto-ransomware (whereby criminals seize computer networks and encrypt the contents until the victim pays a ransom) is rising rapidly. Finally, the report pointed to the late 2015 attack on the Ukrainian energy sector as evidence that "critical infrastructure is worryingly vulnerable."[2]

Cybersecurity is also an arena of geopolitical tension and nation-state gamesmanship. State-on-state cyber espionage is a routine occurrence. Many advanced states have embraced national security doctrines that include the use of offensive disruptive cyber operations not only in response to incoming cyberattacks but also in first-use mode to gain wartime advantages. National security and intelligence organizations build and buy cyber vulnerabilities for possible later use—sometimes resulting in leaks that have serious negative consequences, such as the 2017 WannaCrypt software based on cyber tools stolen from the U.S. National Security Agency (NSA) and used in ransomware attacks targeting thousands of businesses including hospitals and governments.[3]

Software giant Microsoft has openly criticized growing national interest in cyber arsenals and called for a "Digital Geneva Convention." After the WannaCrypt ransomware attacks, Microsoft President and Chief Legal Officer Brad Smith stated:

> "[T]his attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability

[1] "Kapersky Lab: 323,000 New Malware Samples Found Each Day," *Dark Reading*, Dec. 7, 2016, http://www.darkreading.com/vulnerabilities---threats/kaspersky-lab-323000-new-malware-samples-found-each-day/d/d-id/1327655

[2] "Kapersky Security Bulletin 2016. Review of the year. Overall statistics for 2016," Kapersky Labs, Dec. 14, 2016, https://securelist.com/kaspersky-security-bulletin-2016-executive-summary/76858/

[3] Andrew Wagner, "Everything you need to know about the 'WannaCrypt' ransomware attack," PBS News Hour, May 16, 2017, http://www.pbs.org/newshour/rundown/everything-need-know-wannacrypt-ransomware-attack/.

> stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today—nation-state action and organized criminal action."[4]

Efforts at protection have failed to keep pace with the growing threats. National laws and practices with regard to criminal uses of the Internet vary widely. International law does not cover many types of cyber activities, and countries disagree about how to apply foundational documents, like the UN Charter, to the cybersphere. The European Union-crafted Budapest Convention on Cybercrime of 2001, which focuses on law-enforcement cooperation against cyber criminals, remains politically controversial particularly because some states, such as Russia and India, think it infringes on national sovereignty.

States disagree about fundamental issues such as freedom of access to information versus state control of political content, the limits of sovereignty in the cybersphere, and governance of the Internet. Governance is further challenged at all levels by the fact that most of the Internet's underlying architecture is owned and operated by private industry, whose interests and priorities differ from those of governments.

Fights over Internet governance exemplify these complex challenges. Starting in the 1990s, the United States was at the forefront of a group of states trying to transition responsibility for some core Internet functions, such as administration of domain names and Internet Service Provider (ISP) addresses, from the U.S. government to a non-profit corporation overseen by a multi-stakeholder organization. Russia and China organized another group of states that wanted to turn over Internet governance to a UN body, such as the International Telecommunication Union. The Internet Corporation for Assigned Names and Numbers (ICANN) completed its transition from working under a U.S. government contract to providing oversight in a multi-stakeholder process coordinated by the Internet Architecture Board (IAB) in 2016, but controversy continues in the UN Internet Governance Forum about national representation in Internet governance structures.

International efforts to reduce cybersecurity risks have been underway since the late 1990s. Russia introduced the first UN resolution on this topic in 1998. The OSCE and the Shanghai Cooperation Organization are the two most active regional organizations. The North Atlantic Treaty Organization's (NATO) Tallinn Manual process to assess the applicability of the international law of armed conflict (LoAC) to cybersecurity can also be considered a multilateral norm-building effort even if it only includes members of one alliance system; thus, it presumably cannot have any direct influence on countries that are not involved in that process.

[4] Brad Smith, "The need for urgent action to keep people safe online: Lessons learned from last week's cyberattack," Microsoft website, May 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

States are working to develop norms and confidence-building measures (CBMs) to create more predictable and safer behavior around cybersecurity issues. CBMs aim to build trust among stakeholders and avoid conflict and miscalculations by increasing transparency and information sharing, while norms provide ideal standards for behavior that state or non-state actors are encouraged to follow. They often comply with these "rules of the road" for moral reasons or to be viewed in a positive light in the international community, and violators can be shamed or face worse consequences. Unlike legally binding arms control agreements that constrain capabilities or behavior, norms and CBMs are voluntary forms of cooperation. Therefore, they typically lack detailed rights and obligations, and agreed ways to verify compliance, resolve disputes, and respond to violations,

Multilateral cyber norm-building efforts

The two most important efforts to establish norms of behavior in cyberspace have been the UN Group of Governmental Experts (GGE) process to develop voluntary norms of behavior in cyberspace and the Organization for Security and Cooperation in Europe (OSCE) work to develop voluntary, practical confidence-building measures (CBMs) to reduce risks of conflict. Both stem from the realization that no state will be able to provide national cybersecurity without international cooperation given the cross-border nature of the Internet itself. The United States and the Russian Federation, two of the states that are far apart on fundamental questions of sovereignty and international law, have been members of all of the GGEs and are standing members of the OSCE. The People's Republic of China, which takes a similar view to Russia, also participated in the GGEs but is not an OSCE member.

Since 2004, there have been five UN GGEs on Developments in the Field of Information and Telecommunications (ICTs) in the Context of International Security. GGEs are typically composed of 15 national experts nominated by States, who work under their own recognizance and make consensus reports to the Secretary-General, who delivers their recommendations for approval by the General Assembly. The five GGEs have had mixed results:[5]

- 2004-5: could not reach a consensus with disagreement about how to address state exploitation of ICTs for national security and military purposes.

- 2009-10: agreed on basic principles, such as the need for dialogue, TCBMs, and capacity building.

- 2012-13: agreed on legal principles, including the applicability of international law especially the UN Charter.

[5] "Fact Sheet: Developments tn The Field of Information and Telecommunications in the Context of International Security," UN Office of Disarmament Affairs, July 2015, https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf; and UNODA website: https://www.un.org/disarmament/topics/informationsecurity/.

- 2014-15 (expanded to 20 experts): made substantial recommendations on norms and principles including state sovereignty, TCBMs, the application of international law, cooperation, and capacity-building.

- 2016-17 (expanded to 25 experts): failed to reach consensus on details of applicability of international law, including UN Charter Article 51 on self-defense and LoAC.

The 57-member OSCE is the world's largest security-oriented regional organization. Its mandate includes arms control, protection of human rights, confidence-building measures, press freedom, and fair elections. The OSCE Secretariat's Transnational Threats Department works with member states on cybersecurity cooperation in tandem with the rotating national OSCE chair. Work has been ongoing since 2011, when the organization first decided to hold a conference to explore a possible OSCE role in strengthening cybersecurity. The OSCE as a whole has taken three sets of decisions since then:

- 2012: decided to draft CBMs to "enhance cooperation, transparency, predictability, and stability to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs."[6]

- 2013: adopted 11 CBMs on information sharing, national legislation, and the development of contact points.[7]

- 2016: adopted five additional CBMs, including national reporting of vulnerabilities discovered, cooperation on protection of national and transnational critical infrastructure, and the development of protected channels of communications for preventing risks of conflict stemming from the use of ICTs.[8]

The GGE and OSCE efforts differ in important ways. As a global effort, the GGE recommendations have been approved by the UN General Assembly and thus by all 193 states in the United Nations. These high-level political commitments are couched in vague terms and do not proscribe how states are to achieve the recommendations. The OSCE, being a regional body, has taken a more bottom-up approach and focused on practical steps to improve cybersecurity cooperation in order to prevent misunderstanding and conflict.

Both the GGE and the OSCE recommendations are voluntary, although the OSCE's wording tends to be more directive. The GGE uses language such as "states should consider" and "states could" rather than language committing states to certain actions. By contrast, the OSCE's language is lighter on "should" and heavier on "will" and "shall," although its agreements are also voluntary.

For example, the 2013 GGE report (Section IV, para 26c) states: "States *should consider* exchanging information on national points of contact, in order to expand and improve existing

[6] "Permanent Council Decision 1039," Organization for Security and Cooperation in Europe (OSCE) website, April 26, 2012, http://www.osce.org/pc/90169.
[7] "Permanent Council Decision 1106," OSCE website, Dec. 3, 2013, http://www.osce.org/pc/109168.
[8] "Permanent Council Decision 1202," OSCE website, March 10, 2016, http://www.osce.org/pc/227281.

challenges of communication for crisis management, and supporting the development of early warning mechanisms."[9] By contrast, OSCE CBM 8 directs that: "Participating States *will nominate* a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. [They] will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and coordinate responses to enable a direct dialogue" and "update contact information annually … ."[10]

The United Nations effort by its nature is more transparent and highly political, while the OSCE works largely in closed sessions with less public scrutiny. Of these two cyber norm-building efforts, the GGE process has been more contentious. Russia and China have been trying to advance their national agendas by building a coalition of developing countries that are increasingly vocal about cybersecurity concerns that cut across many issues examined at the United Nations.

The 2013 GGE report set out agreement on several high-level principles including:

- Sovereignty applies to ICT activities and infrastructure inside a state.
- International law, including the UN Charter, is applicable to cyberspace.
- Respect for human rights is required within the cybersphere.[11]

These principles are somewhat controversial and contradictory in ways that get exacerbated by modern ICTs. Sovereignty is commonly understood to mean "supreme authority within a territory," but some political systems and philosophers conceive of sovereignty in ways that are more absolute and unlimited than others do.[12] Sovereign states can make their own choices about their internal political, economic, social, and cultural systems, but they cannot do whatever they want without regard for the effects on others. The 1948 Universal Declaration on Human Rights created a set of 30 politically, but not legally, binding constraints on how sovereign governments should treat their own citizens, including recognizing their right to "seek receive and impart information and ideas through any media and regardless of frontiers."[13]

Russia, China and a handful of other states are adamant that national governments should be able to control information within their borders. They often refer to information spread by political opponents as a "weapon" that can weaken national unity, core values, and government legitimacy. They have been trying to build support in the United Nations for a treaty-based approach to what they call "information security." It would include the right for states to police content and political discourse within their borders, thus establishing a more state-centric model for Internet governance than currently exists. Such a treaty would up-end the Western insistence on freedom of information as a basic human right. It would also contradict the West's preference for multi-stakeholder governance in the cybersphere.

[9] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98*, UN General Assembly, June 24, 2013, (hear after GGE 2013 report) http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

[10] "Permanent Decision Document 1106," OSCE, op cit.

[11] GGE 2013 Report, op cit.

[12] Daniel Philpott, "Sovereignty," *Stanford Encyclopedia of Philosophy,* at: https://plato.stanford.edu/entries/sovereignty/.

[13] Universal Declaration of Human Rights: http://www.un.org/en/universal-declaration-human-rights/.

The Western view has been that norms should focus on protecting the Internet's global infrastructure and operations rather than on governments' control over what their own citizens can see. Nevertheless, the Tallin Manual does identify cyber-operations meant to achieve regime change or coercive political interference as violations of the UN Charter's prohibition on intervention in the internal affairs of sovereign states. This would include using online media to spread fake news or manipulate public opinion right before an election or tampering electronically with the electoral system itself.[14] Nations, however, have different ideas about what sort of information (such as propaganda or false information) crosses the line to malicious behavior in the cybersphere.

Another set of controversial questions involves if and how international legal constraints on threats and use of force apply in the cyber realm. The UN Charter prohibits the use of force without Security Council authorization, except in self-defense or collective defense against armed attack. China and many other countries maintain that the attack must be imminent or have already occurred, while the United States has increasingly argued for the right of preventive self-defense.[15] There is no agreement about how severe a cyber event must be to constitute an "armed attack" beyond the general understanding that its scale and effects must be comparable to non-cyber operations that would justify the defensive use of force. Nor have China and some other countries accepted that the LoAC applies to cyberspace as it does to the physical domain. While China supports the humanitarian objectives of the LoAC, Chinese experts have suggested that cyber-specific rules should be developed to protect civilians during conflict.[16]

China accepted the principle that international law applies in cyberspace during the 2013 GGE, but its more restrictive interpretation nearly blocked consensus at the 2015 GGE. Disagreement about the definition of "self defense" and an "armed attack" in the cybersphere and the right of a state to respond to cyber attack using "countermeasures," such as sanctions, became insurmountable hurdles (positions that Russia also held) to consensus at the 2016-17 GGE.

Other developing countries have been increasingly vocal about their fears that Western nations, the United States in particular, are seeking to maintain military supremacy by claiming that international law provides for unlimited right of self-defense against asymmetrical cyber challenges. In a harsh statement to the UN General Assembly following the GGE's failure to reach consensus, Cuba accused "some nations" of "seeking to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions, including military action, by States claiming to be victims of illicit use of ICTs."[17]

[14] Michael N. Schmitt, ed., *Tallin Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013, pp. 44-5.

[15] Julien Ku, "Forcing China to Accept that International Law Restricts Cyber Warfare May Not Actually Benefit the U.S.," *Lawfare*, Aug. 25, 2017, https://lawfareblog.com/forcing-china-accept-international-law-restricts-cyber-warfare-may-not-actually-benefit-us.

[16] Kimberly Hsu, "China and International Law in Cyberspace," U.S.-China Economic and Security Review Commission Staff Report, May 6, 2014, https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.

[17] "71 UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security," Cuban Government press release, June

The United States and Western states have countered that applying international law would help reduce the risks of conflicts by establishing how states can and cannot legitimately respond to malicious cyber activities. Such responses, in the Western view, could include economic sanctions and even a cyber response if the action was deemed hostile.

The breakdown of consensus in 2017 at the GGE has ended the work on cybersecurity in the First Committee (the UN body charged with peace and security issues) at least for now. Michele Markoff, State Department deputy coordinator for cyber issues and the U.S. representative to the GGEs, said earlier in 2017 that the Trump administration's focus would be on "consolidating" gains rather than pursuing additional cyber norms.[18] After the last acrimonious GGE session in 2017, there has been no further agreement about what, if any, continuing role the United Nations should play in norm-setting. As of early 2018, there are no plans for a follow-on GGE or any other UN work on cybersecurity.

The GGE's struggles with applying principles of international law to actions in the cyber domain have not been echoed in the OSCE process, largely because the OSCE has chosen to focus on practical elements of transparency and cooperation rather than on trying to reach consensus on the larger political issues surrounding norm-setting. Nevertheless, the combination of growing political tensions between Russia and the United States and leadership changes in key countries likewise have made the OSCE's work on cybersecurity cooperation more difficult since 2013. The OSCE's focus is now firmly on implementing already agreed TCBMs rather than pushing for new or more explicit TCBMs.

Common themes: Sharing information, protecting critical infrastructure, and reducing risks of conflict

Efforts to consolidate gains could have the most impact if they revolve around themes that received broad support in both the GGE and the OSCE processes. The principles, norms, and TCBMs in these documents represent political commitments that will be difficult to disregard even though they are voluntary and vague. Blatantly violating the already agreed-upon norms, particularly those endorsed in both forums, would have political costs. At the same time, joint projects to implement some of the cooperative ideas that found support in both forums could have practical benefits.

The GGE recommendations and the OSCE CBMs both address the need for *improved communications and information sharing*, including about national contact points, classification systems for cyber events, and methods for assessing the severity of cyber incidents. Both processes underscore the need for *cooperation to prevent and respond to cyber incidents,*

23, 2017, http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

[18] Joseph Marks, "New International Cyber Rules Likely Off the Table for UN Expert Group," *NextGov*, Feb. 6, 2017, http://www.nextgov.com/cybersecurity/2017/02/new-international-cyber-rules-likely-table-un-experts-group/135193/.

particularly those stemming from the actions of criminals and terrorists. Both processes identify the importance of *cooperative protection of national and transnational critical infrastructure.* Both processes also call for *capacity building*, including promoting global Internet access and developing cyber expertise in countries lagging behind in the digital revolution. A chart comparing the relevant GGE and OSCE language on these themes is in Appendix A.

Information sharing and communications. The GGE is primarily concerned about the need for improved communications, specifically for crisis communications and early warning regarding potential incidents, while the OSCE seeks to improve communication across the board as a prerequisite to cooperation on a wider range of cybersecurity challenges.

The GGE encourages states to share more information about cybersecurity without specifying what current or new mechanisms they should use, while the OSCE is more specific. Its CBM 5 says: "States will use the OSCE as a platform for dialogue, exchange of best practices … including effective responses to related threats."[19] This makes sense, given that GGEs are ad hoc rather than standing bodies within the UN system. The OSCE is an established organization with a Secretariat, regular meetings, and established procedures for information sharing that can easily be adapted to this purpose.

On points of contact, both the GGE and the OSCE see their establishment as a first step to improving information sharing, but the OSCE considers the matter more urgent. Establishing points of contact for communications between governments on cyber issues may seem trivial and easy, but it is actually quite important and more complicated than it seems. Even states with well-developed and sophisticated national cybersecurity policies and organizations still have difficulty with coordination and lines of authority regarding prevention and incident response. Many nations have the added problem of securing open and timely communications between the private sector, particularly software and Internet provider companies, and national governments. Assigning points of contact, with authority to share certain information, could not only help improve international cooperation but also help clarify internal state procedures and accountability.

The OSCE is helping less advanced states figure out who should be their national points of contact by holding workshops to elucidate how countries are organizing their cybersecurity activities (if at all), explore linkages with computer emergency response teams (CERTs), etc. This in turn should help those states with establishing a chain of command for cybersecurity activities, as points of contact given authority for transparency measures and cooperative actions will necessarily have to interact with various departments and organizations with other cybersecurity responsibilities, such as setting policies, ameliorating the effects of cyber intrusions, and developing network protections. In other words, working to establish a point of contact requires working to establish lines of authority for cybersecurity *within* a national government—something that many less Internet savvy countries have been struggling to do.

The OSCE 2013 CBM recommendations also encourage sharing other types of information about national practices.

[19] "Permanent Decision Document 1106," OSCE, op cit.

- CBM 2 states: “Participating States will voluntarily facilitate cooperation among the competent national bodies and exchange information in relation with security of and in the use ICTs.”
- CBM 4 states: “Participating States will voluntarily share information on measures they have taken to ensure an open, interoperable, secure, and reliable Internet.”
- CBM 9 addresses the problem of lack of agreed terminology, instructing States to, “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.”[20]

OSCE diplomats hope this will help prevent misunderstandings and provide models for less advanced states inside and outside the region to emulate. The OSCE shared some lessons learned through its work on CBMs at the first meeting of the Organization of American States (OAS) working group on cooperation and confidence building in cyberspace on March 2, 2018.

The GGE reports make some similar recommendations. For example, the 2015 GGE urged states to adopt national processes to classify incidents “in terms of scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.” It also encouraged states to share information on “national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT enabled infrastructure.”[21]

Cooperation on threats and incident response. The OSCE has a direct mandate to work on preventing risks of conflict in Europe. The GGE on ICTs was created under the UN First Committee, which deals with international peace and security. Thus, it also had a direct mandate to address conflict prevention.

The 2015 GGE report urges state cooperation to develop and apply “measures to increase stability and security” and to prevent ICT practices that are harmful or might pose threats to international peace and security. In one of the strongest passages in the report, it underscores that states “should not knowingly allow their territory to be used for wrongful acts using ICTs.”[22]

The GGE reports place a heavy emphasis on cooperation regarding the use of the cybersphere by criminals and terrorists. It is often more comfortable for governments to cooperate against non-state actors than it is for them to address security problems created by their own actions. The OSCE reflects broader imperatives for cooperation to combat all vulnerabilities and threats and respond to and recover from incidents. The OSCE discussions stressed the transnational nature of threats (in that many malicious cyber activities “jump” from one state to another) and the fact that some nations are better equipped to deal with incidents, thus have the ability to assist those with lesser capabilities.

The 2015 GGE report calls upon states to “intensify cooperation” against criminal or terrorist cyber activities, implement measures to exchange information and cooperatively prosecute perpetrators, and assist with response and recovery measures if called upon to do so by a

[20] “Permanent Council Decision 1106,” OSCE, op cit.
[21] GGE 2015 Report, op cit.
[22] GGE 2015 Report, op cit.

victimized state. It also recommends that states “respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account the due regard for sovereignty.”[23]

The 2016 OSCE decision document calls for states to develop “non-public” communications channels to discuss incidents in order to reduce misperception, dampen tensions, and avoid crisis escalation. It also instructs states to clarify the technical, legal, and diplomatic mechanisms that individual states can use to respond to requests for information and assistance regarding an incident.

OSCE CBM 16 urges member states to be proactive about sharing information to prevent cyber attacks. It directs: “Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing cooperation and transparency within the OSCE region.”[24]

Critical infrastructure. The most recent GGE 2015 report and OSCE 2016 guidelines doubled down their focus on critical infrastructure, *emphasizing the centrality of cooperative protection of critical infrastructure, especially infrastructure that crosses national borders.*

Protecting critical infrastructure from cyber attack has been an overriding concern for many national governments for decades. Electricity grids (especially nuclear power plants), water supply (i.e. dams), transportation grids, hospitals and health care systems, communications networks, and the “core” of the Internet (including physical infrastructure such as fiber optic cables and satellites; Internet routing; and the domain name system[25]) are widely considered critical infrastructure.

The 2013 and 2015/2016 GGE and OSCE processes have focused on critical infrastructure as a crucial area for multilateral cooperation, especially regarding potential malicious cyber activities by non-state actors such as cyber criminals and terrorist organizations. A further concern of international diplomats is that disruptions of a nation’s critical infrastructure might lead to conflict, particularly during periods of heightened tension between states.

That said, there is no internationally recognized definition of critical infrastructure and such designations vary from state to state. Eviatar Matania, head of Israel’s National Cyber Bureau, succinctly characterized this problem. “The norm of ‘do not attack critical infrastructures’ sounds great,” he said, but “[t]he definition in every nation is different. Some will define everything as critical.”[26]

[23] GGE 2015 Report, op cit.

[24] “Permanent Council Decision 1202,” OSCE, op cit.

[25] There is no agreed definition of what makes up the “core” or “backbone” of the Internet, although there is increasing international interest in trying to define both infrastructure and functions of the Internet that provide global connectivity and thus should be “off limits” for disruption and attack.

[26] Joe Uchill, “Israel cyber head: US-backed cyber norms too broad,” *The Hill*, Sept. 13, 2016, http://thehill.com/policy/cybersecurity/295651-israel-cyber-head-us-supported-cyber-norms-too-broad.

The 2015 GGE report encourages states to share information about how they categorize and protect critical infrastructure, including national law and policies. In particular, the GGE notes the need for cooperation to address incidents that involve "ICT enabled industrial control systems." It suggests that states develop a "repository of national laws and policies for the protection of data and ICT-enabled infrastructure" and share as much as possible about them.[27]

The OSCE also calls upon states to share their views of what constitutes critical infrastructure. It goes further than the GGE by encouraging regional and sub-regional cooperation to protect transnational critical infrastructure. CBM 15 recommended that states should work together to "discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies," including "[d]eveloping, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure."[28]

During the GGE and OSCE discussions, some states raised the possibility of identifying types of critical infrastructure that should be "off limits" to cyber attacks by nation states, including nuclear power plants and the "core" protocols and infrastructure of the Internet. The Netherlands, Germany, and Switzerland were key initiators of this concept. The issue was never formally taken up by either body, though, due to lack of agreement about what critical infrastructure to single out, as well as whether such a ban on offensive cyber action could be implemented.

Challenges and opportunities for progress

Neither the UN nor the OSCE processes can, in and of themselves, implement their recommendations—that is up to individual states. Much can be done, though, to encourage implementation of agreed-upon norms through bilateral, multilateral, and multi-stakeholder efforts. The mistrust between the larger state players—China, Russia, and the United States—creates both an opportunity and a need for Middle Powers such as Germany, the Netherlands, Switzerland, Australia, and Canada to demonstrate creative leadership.

Even the most skilled diplomats will not be able to turn vague principles and recommendations for cybersecurity cooperation into agreements to do, or not to do, specific things on their own. Representatives of companies that own or operate key parts of the ICT infrastructure should be included in these discussions, along with some private sector cybersecurity service providers. Academic experts who understand the many complex interactions between technology and legal/policy issues can also make important contributions.

With the GGE process currently stalled, the OSCE is the most promising venue for multilateral work on cybersecurity cooperation. Because it meets regularly, it can encourage, assist, and track actions by member states. It and other relevant regional organizations such as NATO, the European Union, the OAS, and the Association of Southeast Asian Nations (ASEAN) can help neighboring states discuss how vague principles apply to specific situations, particularly when

[27] GGE 2015 Report, op cit.

[28] "Permanent Council Decision 1202," OSCE, op cit.

difficult value trade-offs are unavoidable. They can also support joint projects that assess different ways of implementing agreed recommendations.

The OSCE could reach back into its own history for ideas about promoting constructive dialogue on the application of agreed principles to specific situations. In the 1975 Final Act of the Helsinki Conference on Security and Cooperation in Europe, 35 NATO and Warsaw Treaty Organization countries and non-aligned states agreed on a more detailed interpretation of what was meant by ten major principles of international law. Although some of these norms were still violated by some signatories, the process of participating in their development, application, and adjudication does seem to have had a positive effect on all states' behavior over time. This forum continued meeting when geopolitical tensions rose and superpower arms control negotiations broke down during the early years of the Reagan administration. The 1986 Stockholm Accord contained an extensive set of pragmatic transparency and confidence-building measures that reduced misperceptions and increased conventional stability in Europe. More importantly, Soviet leader Mikhail Gorbachev's internalization of the Helsinki Decalogue was an important factor in his decisions to respond non-violently when the Baltic states declared their independence from the U.S.S.R. and several Eastern European countries ended their subservient relationship to it.

One of the OSCE's main activities in recent years has been election assistance and monitoring. It would therefore be a natural forum to discuss what types of information-related activities are appropriate for foreign governments and non-profit organizations to undertake in support of civic engagement and media freedom, as well as what crosses the line into unacceptable interference in other country's politics and social cohesion. This topic would undoubtedly be extremely controversial, so it is important for the OSCE to pursue some more practical project to aid norm implementation at the same time.

One foundational area for further cooperation is the development of *agreed terminology* (by the OSCE) and *processes to classify incidents and assess their severity* (by the GGE). This would be useful for a number of purposes, including clarifying which cyber events are comparable in scale and effects to an armed attack and which have relatively minor disruptive effects or are intended for espionage or criminal theft of information.

Even in the United States and other countries with advanced cyber capabilities, alarmist terms like "cyber attacks" and anodyne ones like "cyber incidents" get applied indiscriminately to a wide range of different phenomenon, some much more serious than others. There is no standard way of differentiating among various uses of ICTs to steal information or disrupt operations, and each of the more common classification systems has important shortcomings. OSCE CBM 9 urged states to share their "list of national terminology related to security of and in the use of ICTs." If states could go further to agree on a common classification system to use, that would facilitate communication and reduce misunderstandings.

The first project for a multilateral, multi-stakeholder cybersecurity group might be to evaluate classification systems and agree on terminology to be used in subsequent projects and potentially recommended for more widespread use. One option is the effects-based taxonomy currently being developed at the University of Maryland's Center for International and Security Studies at Maryland (CISSM). It considers three rings of effects: (1) the primary effects on the target organization's ICT capabilities; (2) the secondary effects on that organization (e.g. impacts to the balance sheet, reduced stock price, damaged reputation); and (3) the second-order effects on other entities who rely on that organization for goods or services (e.g. supply-chain disruptions, interruptions in power or transportation, and environmental damage or loss of human life). Primary effects can be either disruptive or exploitative depending on whether the attacker's main objective was to interfere with an organization's operations or steal information. Disruptive events can be sub-divided into five comprehensive and mutually exclusive categories depending on the part of an organization's ICT infrastructure that is most seriously impacted, regardless of what tactic or technique was used to accomplish that effect. Exploitative events can also be sub-divided into five categories depending on the location from which the information was stolen.[29]

The severity of a cyber event depends not only on the type of event but also on the type of organization affected and its relationship to other entities. For example, external denial-of-service attacks are typically less severe than physical attacks on SCADA control systems used in modern manufacturing plants, but a campaign that completely overwhelmed the SWIFT banking code system's ability to process financial transactions for several hours would probably have more severe primary, secondary, and second-order effects than a physical attack on one machine at a toy manufacturer. CISSM's Cyber Disruption Index provides a tool to estimate the scope, magnitude, and duration of five different categories of cyber incidents that have or could disrupt different parts of an organization's ICT infrastructure so that business leaders and policymakers can set priorities for protection and coordinate incident response.[30] CISSM's cybersecurity risk assessment framework will also include a Cyber Exploitation Index to measure the effects of different ways of stealing information.

Cooperation to prevent the worst sorts of cyber attacks is another area where further cooperative work might be productive. Elaborating what *critical infrastructure—both at the national and transnational level—should be protected*, and subject to collaboration regarding vulnerabilities, threats, and response, would be a second fruitful area for multilateral, multi-stakeholder discussions. Different states have different views on what is considered national critical infrastructure. Further, no state wants to provide a specific "target list" of critical infrastructure for potential adversaries to target or to reveal their precise vulnerabilities. Still, there are mutual interests regarding protection of critical infrastructures that lend to the understanding that cooperation in this area is not only useful but necessary.

Most, but not all, countries maintain that LoAC does not protect some types of critical infrastructure (such as electric grids or transportation routes) during war if a case can be made regarding military necessity and "proportionality" (meaning losses of civilian life and property incidental to the attack must not be "excessive" in relation to the military advantage gained).[31] However, some states have been seeking agreement that certain types of critical infrastructure

[29] Charles Harry, "A Proposed Hierarchical Taxonomy for Assessing the Primary Effects of Cyber Events: A Sector Analysis 2014-2016," CISSM, February 2018, http://www.cissm.umd.edu/publications/proposed-hierarchical-taxonomy-assessing-primary-effects-cyber-events-sector-analysis.

[30] Charles Harry and Nancy Gallagher, "Categorizing and Assessing the Severity of Disruptive Cyber Incidents," CISSM, April 2017, http://www.cissm.umd.edu/publications/categorizing-and-assessing-severity-disruptive-cyber-incidents.

[31] "Law of Armed Conflict (LOAC), 4 Basic Principles," *LOACblog.com*, https://loacblog.com/loac-basics/4-basic-principles/.

should be considered "off the table" for attack during both peacetime and conflict because the potential harm to noncombatants in the target country and other states could be unjustifiably high. A cyber attack on a nuclear power plant capable of causing a core meltdown and releasing long-lasting radioactive material might be one type of cyber attack that all OSCE members, and even all states, could agree to rule out.

Transnational Internet infrastructure (e.g. data relay hubs, the domain name system) is another type of critical infrastructure that has been gaining support for special protections in Track 1.5 discussions that bring together government officials and non-governmental experts and in conversations on the margins of the GGE and OSCE. Several states, including the Netherlands and Germany, continue to be interested in moving in this direction. In a 2015 study, the Netherlands Scientific Council for Government Policy (a government advisory body) recommended that the "core" of the Internet be considered a "public good" and deemed a "neutral zone" for conflict.[32] There is an opportunity for further research and discussion among experts to flesh out how this approach might be structured technically, legally, and politically.

There is no universal definition of what constitutes the "core" of the Internet, nor any agreement on terminology (i.e. some experts refer instead to the "Internet backbone"). The Global Commission on the Stability of Cyberspace (GCSC), a group of independent scholars and experts funded in part by the Netherlands, has issued a "Call To Protect The Public Core Of The Internet," explaining its understanding of the core as including "Internet routing, the domain name system, certificates and trust, and communications cables."[33] Even this definition remains somewhat vague. For example, there are many different kinds of certificates of identity at different levels of Internet activity, only some of which are essential to the functioning of the Internet as a whole. Although the bulk of Internet traffic continues to travel via fiber optic cables, increasingly Internet traffic is being routed through satellite communications. This reliance on satellites, particularly in the developing world, will grow as companies move closer to establishing constellations of satellites specifically designed for web traffic in remote areas. Therefore, there is work to be done in establishing an agreed definition of the Internet "core" as well as agreed approaches to protection.

CISSM's cyber risk assessment framework could be used by members of a multilateral multi-stakeholder cybersecurity group to think through the implications of defining the" public core" of the Internet in different ways. The widely accepted Open System Interconnection (OSI) model of how applications communicate over a network identifies seven "layers" of machine interactions that constitute "the Internet," three of which have the most relevance to cybersecurity (Layer 1, 3, and 7). Multilateral and multi-stakeholder cooperation to protect the "public core" would take different forms depending on whether it focused solely on Layer 1 (the physical infrastructure) or also included some functions at Layer 3 (networking) and Layer 7 (applications). If participants were able to agree on at least some aspects of the "public core" of

[32] Dennis Broeders, "The public core of the Internet: An international agenda for Internet governance," The Netherlands Scientific Council for Government Policy, 2015, Amsterdam University Press, https://en.aup.nl/books/9789462981959-the-public-core-of-the-internet.html.
[33] "Call to Protect the Public Core of the Internet," Global Commission on the Stability of Cyberspace," November 2017, https://cyberstability.org/wp-content/uploads/2017/11/call-to-protect-the-public-core-of-the-internet.pdf.

the Internet that deserved special protection, then they could use the risk assessment framework to determine what types of cyber attacks targeted at those components would have the most severe secondary effects. This could lead to a greater willingness to share information about threat actors, vulnerabilities, protection methods, and consequence management. It might even lead to agreement that some categories of attacks could not be justified under the LoAC except, perhaps, under very narrow circumstances.

A third area where international discussions could be productive is *clarifying what types of information states should be willing to share* to prevent or respond to cyber attacks by criminals, terrorists, or other non-state actors. The GGE and OSCE are not alone in urging more information sharing. A 2017 CISSM survey found references in the public domain to 196 such agreements involving 116 countries. Few texts of these agreements are public. Those that are use vague language. This makes it difficult to ascertain how much cyber information sharing is actually occurring, let alone whether the information that is shared actually helps to reduce threats, increase resilience, and aid recovery.[34]

Anecdotal evidence suggests that within NATO, countries with more advanced cyber exploitation and disruption capabilities hesitate to share information with allies who are less comfortable with offensive cyber activities. Reluctance to reveal what one knows about threat actors and software vulnerabilities is even more pronounced within regional organizations like the OSCE that include a more diverse set of countries with more complicated relationships. Information sharing between governments and private sector companies is also problematic. Rather than continue to talk in the abstract about the benefits of information sharing, it might be more productive to think through, from different perspectives, a set of scenarios requiring decisions about what information to share with whom under what conditions and for what purposes.

The CISSM risk assessment framework can be used to help stakeholders with a mix of common and conflicting interests think through tradeoffs that would influence information-sharing choices. In one tabletop exercise that CISSM conducted involving four neighboring countries, the one that started with the least interest in information sharing became progressively more motivated to share specific types of information to avoid being blamed for an attack undertaken by a non-state actor. The country that started as the strongest proponent of sharing decided for economic reasons only to reveal a control system vulnerability to its ally, but a series of chance events led it to be contaminated by a nuclear meltdown. This type of exercise could easily be used to explore information sharing among different agencies in the same country or between government officials and private sector organizations.

[34] Theresa Hitchens and Nilsu Goren, “International Cyber Sharing Agreements,” October 2017, Center for International and Security Studies at Maryland, http://www.cissm.umd.edu/sites/default/files/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf.

Conclusions

Despite their slow pace and sometimes "one step forward, two steps back" progress, efforts at the multilateral level to craft norms and TCBMs in the cybersphere are making headway. Such norms and agreements have the potential to not only improve the safety and security of the cybersphere but also to reduce risks of conflict that undercut international peace and security. Further progress, however, will require both continued cooperation and compromise by the major powers, especially China, Russia, and the United States as leaders of state groups with clashing ideologies regarding the definition of cybersecurity.

Other technologically advanced powers also have an important role to play. These nations can serve as a bridge between the "Big Three" and can also support and encourage nongovernmental and academic work to elucidate the technical, legal, and political challenges and opportunities for further progress.

That said, norms and voluntary TCBM agreements are only useful if they are implemented. Thus, there is a need for more detailed work to help states understand the agreements that have been reached to set up national practices that allow their implementation. The efforts of the OSCE to establish mechanisms for communication and cooperative activity is one example of such necessary work, which could be a model for other regional organizations. Efforts by the GCSC are also to be applauded, as the Commission is bringing together international experts, academics, and lawyers from around the globe to address key issues in cyber norm-setting.

The private sector also has a role to play and must be encouraged by governments to do so. So far, with the exception of Microsoft, the ICT industry has been notable only for its absence in multilateral discussions of cyber norms. Unfortunately, many Internet companies see governments as an adversary—sometimes for good reasons, including lack of government understanding of the cybersphere, heavy-handed regulation, and the efforts of national security organizations to compromise private sector tools and networks for their own uses. This situation must be remedied to ensure a safe, secure, and sustainable Internet. There is a desperate need for bridge building between the public and private sector; both governments and nongovernmental organizations must put more effort into this.

A focus on the Internet "core" and transnational infrastructure is a logical starting point for further agreement. Disruption of the global Internet via cyber attack on infrastructure and critical functions would have serious negative effects for all states. Disruption of transnational energy grids could result in widespread civilian harm and negative economic consequences for many nations. While work on the protection of the Internet "core" is amendable to multinational efforts, regional organizations would be better placed to address questions of transnational infrastructure, as such infrastructure is regional in many sectors (e.g., energy grids, fresh water management, and railroads).

Above all, states must not give up hope on the value of diplomatic efforts. The ongoing rush by many states to obtain offensive cyber capabilities for potential use in conflict (either internal or external) creates risks not only to international security but also to national security. Cyber tools developed or purchased in secret to exploit adversary networks always carry the potential for "friendly fire." This is because most cyber networks rely in some fashion on private sector infrastructure. In many cases, hoarding an offensive cyber tool means that a government is leaving open its own networks to a vulnerability. In the cyber world, such vulnerabilities do not stay secret for long.

While states may ultimately decide that some form of cyber offense is required for national security, such decisions should not be made without weighing their potential consequences (including second- and third-order consequences) and considering what benefits for national cybersecurity might be obtained from diplomatic agreements that put restraints on all state activities.

The very nature of the cybersphere is connectivity. That connectivity makes it impossible for any state to ensure its own cybersecurity without the cooperation of other states. It also means that the actions of one state can have tsunami-like effects at a global level. There are fundamental mutual interests in a global regime that improve the level of cybersecurity for all. Norm-setting and the development of TCMBs may be voluntary, but they lay a foundation for such a future regime and should not be disregarded lightly.

About the authors

Theresa Hitchens is a Senior Research Associate at the Center for International and Security Studies at Maryland (CISSM). Prior to joining CISSM, Hitchens was the director of the United Nations Institute for Disarmament Research (UNIDIR) in Geneva from 2009 through 2014. Nancy Gallagher is the Director of CISSM and a Research Professor at the University of Maryland's School of Public Policy.

Appendix

The following tables provide a comparison of the language used in cybersecurity recommendations by the United Nations Group of Governmental Experts (GGE) and Organization for Security and Cooperation in Europe (OSCE) in overlapping areas that have received broad support.

Peace and Security

GGE Recommendations	OSCE Recommendations
2015, Section III, para 13a: "States should 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." 2015, Section III, para 13b: "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." 2015, Section III, para 13c: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."	2016, CBM 12: "Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges … to investigate the spectrum of cooperative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs." 2016, CBM 13: "Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests."

Information Sharing and Communications

GGE Recommendations	OSCE Recommendations
Mechanisms	
N/A	2013, CBM 5: "States will use the OSCE as a platform for dialogue, exchange of best practices … including effective responses to related threats."[35]
Points of Contact	

[35] Permanent Decision Document 1106, op cit.

2013, Section IV, para 26c: “States should consider exchanging information on national points of contact, in order to expand and improve existing challenges of communication for crisis management, and supporting the development of early warning mechanisms.”	2013, CBM 8: “Participating States will nominate a contact point to facilities pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and coordinate responses to enable a direct dialogue … States will update contact information annually … .”
Other/National Practices	
2015, Section IV, para 16d: “The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure.” 2015, Section IV, para 16d: “States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include … The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.”	2013, CBM 2: “Participating States will voluntarily facilitate cooperation among the competent national bodies and exchange information in relation with security of and in the use ICTs.” 2013, CBM 4: “Participating States will voluntarily share information on measures they have taken to ensure an open, interoperable, secure, and reliable Internet.” 2013, CBM 9: “States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term.”

Threats and Incident Response

GGE Recommendations	OSCE Recommendations
Threat Reduction	
2015, Section III, para 13a: “States should 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.” 2015, Section III, para 13c: “States should not knowingly allow their territory to be	2016, CBM 13: “Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests.”

used for internationally wrongful acts using ICTs." 2015, Section IV, para 18: "The Group reiterates that, given the pace of ICT development and the scope of the threat, there is a need to enhance common understandings and intensify cooperation." 2013, Section III, para 22: "States should intensify cooperation against criminal or terrorist use of ICTs … ."	
Response/Recovery	
2013, Section IV, para 26c: "Enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels and the develop of appropriate new channels and mechanisms to receive, collect, analyze and share information related to ICT incidents, for timely response recovery and mitigation actions." 2015, Section III, para 13d: "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. States may need to consider whether new measures need to be developed in this respect." 2015, Section III, para 13h: "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 the due regard for sovereignty."	2016, CBM 16: "Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing cooperation and transparency within the OSCE region."

Critical Infrastructure

GGE Recommendations	OSCE Recommendations
2013, Section IV, para 26e: "Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among States against disruptions perpetrated by non-State actors." 2015, Section IV, para 16d: "The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include … A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies."	2013, CBM 3: "Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity." 2016, CBM 15: "Participating States, on a voluntary basis, will encourage, facilitate and/or participate in … collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies … Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure." "Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;" "Sharing national views of categories of ICT-enabled infrastructure States consider critical;" "Improving the security of national and transnational enabled critical infrastructure including their integrity at the regional and subregional levels."

Sources:
GGE 2013 Report: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98
GGE 2015 Report: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
OSCE 2013 "Permanent Council Decision No. 1106": https://www.osce.org/pc/109168

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