TOWARDS A SECURE CYBERSPACE VIA REGIONAL CO-OPERATION

Overview of the main diplomatic instruments

DiPLO
www.diplomacy.edu

Geneva Internet Platform

IMPRESSUM

Towards a secure cyberspace via regional co-operation

Published by DiploFoundation (2017)

E-mail: diplo@diplomacy.edu
Website: www.diplomacy.edu

Authors: Vladimir Radunovic and the DiploFoundation team
Editing: Mary Murphy
Maps: Aye Mya Nyein
Layout and design: Viktor Mijatovic
Research commissioned and funded by the Swiss Federal Department of Foreign Affairs (FDFA)

DiPLO
www.diplomacy.edu

Geneva Internet Platform

Contents

Introduction

The paper *Towards a secure cyberspace via regional co-operation* has been prepared by DiploFoundation, in partnership with the Geneva Internet Platform (GIP) and with support of the Swiss Federal Department of Foreign Affairs (FDFA), on the occasion of the second meeting of the 2016/2017 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), held in Geneva in November 2016.

Its intention is to provide an overview of the international dialogue on establishing the norms of state behaviour and confidence-building measures (CBMs) in cyberspace. It offers a comparative analysis of the leading international and regional political documents outlining cyber-norms, CBMs to reduce conflict stemming from the use of ICT, and capacity-building efforts to strengthen co-operation on cybersecurity. Consequently, it discusses how they could further influence each other, and notes several specific directions that further developments could take.

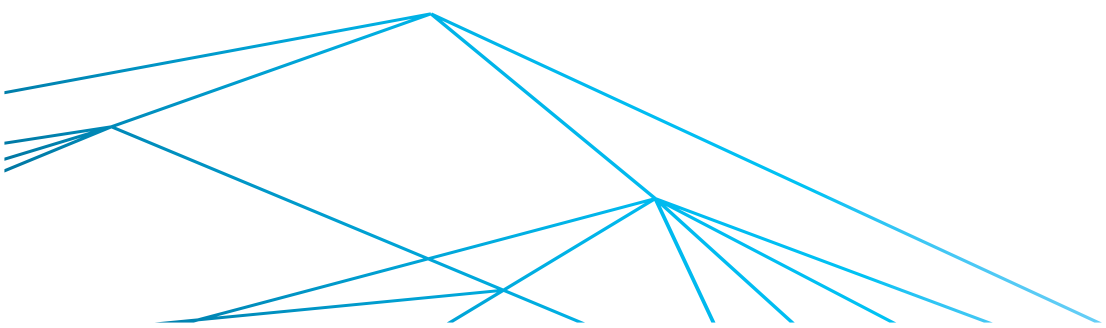
Section 1 offers an insight into the general context related to maintaining peace and security in cyberspace. It presents key challenges with applying existing international law to cyberspace alongside the obstacles introduced to global negotiations by different terminology used by various parties.

Section 2 reviews major international and regional diplomatic initiatives and instruments, with a specific focus on the efforts of the United Nations, the Organization for Security and Co-operation in Europe (OSCE), the Association of Southeast Asian Nations (ASEAN) Regional Forum, and the Organization of the American States (OAS). It also provides a brief overview of other initiatives, such as the efforts of the Shanghai Cooperation Organisation (SCO), the G20, NATO, and Microsoft, among others. It concludes with a non-exhaustive list (and map) of the established bilateral cyber-relations around the world.

Section 3 suggests the classification of various norms and CBMs defined by the UN, the OSCE, ASEAN Regional Forum, and the OAS; compares the specific measures; and suggests their potential positive mutual impact. In addition, it provides a classification of suggested capacity building measures.

The paper is not intended as a comprehensive overview of the topic or a review of all related initiatives; instead, it provides sufficient background information to provoke further debate and analysis.

For comments and suggestions, contact the team at **diplo@diplomacy.edu**



1 Context

1.1 Changing environment

What once might have been a science-fiction scenario – that we, and everything around us, are interconnected – is a reality that benefits everyone: from simple convenience to ubiquitous access to information and knowledge, from automatisation of processes to highly efficient systems. These benefits are accompanied by security threats which are equally sophisticated and ubiquitous: from possible failure of or attacks on the Internet infrastructure (resulting in the inaccessibility of services), to breaches of personal data and misuse and manipulation of information.

Today's Internet – the backbone of the modern digitalised world – works more or less in the same way as it did when it was developed in the 1960s. It was originally designed for use by a closed circle mainly of academics. Communication was open and security was not a concern. Vulnerabilities existed – and still exist – on many levels, but they were not explored or exploited before the Internet's expansion beyond the circle of Internet pioneers.

With the increasing use of the Internet in everyday life and especially in global business, traditional crimes such as fraud, identity theft, and buying illegal goods are now being conducted through the Internet as well. On an organised level, black markets hidden within the 'dark web'[1] allow distribution of and access to various products and services – from viruses and botnets to drugs and weapons – all are just 'one click away' and almost risk-free. A particularly flourishing offer is that of cyber-weapons (e.g. exploits, malware kits, and botnets[2]). Each day, the headlines feature updates about millions of passwords for online services, or the new 'zero-day'[3] exploits – all for sale. The abundance of hacked information and exploits enables the emergence of cheaper and simpler to use, yet more sophisticated malware (such as Trojans or ransomware) and social engineering techniques (such as phishing and spear-phishing), and even cyber-attack services (distributed denial-of-service or DDoS attacks, hacking and defacement, spam and malware distribution) – with customer support. For instance, a smaller botnet can be rented for about €100, or a DDoS attack ordered for less than €50 per day; no specific skills are required except for how to find such offers online. Available, affordable, ready-made, and simple-to-use cyber-weapons, combined with the low risk of prosecution due to anonymity, in turn invite greater interest from various individuals and groups who want to purchase tools and hire services online. In addition, certain security companies – Vupen and Hacking Team are among the most outspoken – have created a lucrative legal business out of discovering vulnerabilities, producing exploits,[4] building them into hacking tools, and finally selling them to security services and governments, among others.

Such developments, coupled with the lack of an efficient global mechanism to combat cybercrime, and a lack of international responsibility for individuals, companies, or states to disclose discovered vulnerabilities instead of misusing them for the proliferation of malicious cyber-tools, have increased the ability of political groups, and states themselves, to carry out cyber-attacks against other states. At the same time, the increasing digital dependence of the entire infrastructure of society – from information, communication, and amusement, business and government services, health and voting, to the security sector and critical services like energy or water supplies – has given rise to the risk that cyber-attacks could have real-world consequences similar to those resulting from natural hazards, terrorist attacks, or kinetic military operations.

1.2 Different terminology

Cyber policy is a policy field in the making. Thus, there is still a lot of terminological confusion, ranging from rather benign differences such as the interchangeable use of prefixes (cyber/e/digital/net/virtual) through to core differences, when the use of different terms reflects different policy approaches. In policy and political discussions about cybersecurity, different organisations and governments use different terminology, but they also view cybersecurity concepts differently.[5]

Differences start from the very terms delineating the field: cybersecurity and information security. The European Union[6] has its Cybersecurity Strategy within which it describes *cybersecurity* as 'safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure'. This understanding of cybersecurity is related to cyber-threats against networks and infrastructure. US laws define *information security* as 'protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction' to provide integrity, confidentiality, and availability.[7] Within its foreign policy endeavours and documents, however, the US government strictly uses the term *cybersecurity* and relates it to

[1] For more about the dark web, refer to: Radunović V (2016) The Dark Web: The good, the bad, and the ugly. Available at https://www.diplomacy.edu/blog/dark-web-good-bad-and-ugly.

[2] Botnets are networks of hijacked personal computers that perform remotely commanded tasks without the knowledge of their owners, and are commonly used to disseminate spam or infections, conduct frauds or distributed denial-of-service attacks. The proliferation of commonly unprotected 'smart devices' within everyday and home appliances carries a particular risk of creating massive and powerful botnets.

[3] 'Zero-day' refers to vulnerabilities discovered by hackers but unknown even to the software producers and antivirus companies.

[4] Exploits are pieces of software code that exploit vulnerabilities to enable inserting advanced malware that can then take over control of computer systems, or do other misdeeds.

[5] The theory of information security provides us with some basic concepts of relevance to defining cybersecurity. This theory refers to the CIA triad: confidentiality prevents the unauthorised disclosure of information (e.g. reading other people's e-mail); integrity prevents the unauthorised change of information (e.g. altering e-payment instructions); availability ensures that the information is available (e.g. ensuring access to e-voting ballots). While most of the terms and concepts used are linked to the CIA triad, they do not share the same meanings.

[6] European Union (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, p.3. Available at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[7] Legal Information Institute (no date) US Code § 3542 – Definitions. Available at https://www.law.cornell.edu/uscode/text/44/3542

protection from cyber-threats and cyber-attacks against critical infrastructure and information systems, while at the same time promoting open Internet and online freedoms.[8]

On the other hand, Russia, China, and their partners from the SCO predominantly use the term *information security* in their foreign policy efforts.[9] More importantly, in their view, the term relates to the strategic control of information and implies a broader understanding of threats including information that could endanger 'societal-political and social-economic systems, and spiritual, moral and cultural environment of states', as defined in the 2015 pact between Russia and China.[10] Within this foreign policy platform, SCO countries strongly opt for clear national sovereignty in the case of cyberspace, which would allow countries to consider content control measures as an 'essential aspect of "information security"'[11] – a concept which conflicts with the open Internet and online freedoms promoted by the USA and the EU.

Human rights communities have also tried to offer a definition of cybersecurity, which suggests that it should be about people rather than about systems: it is a matter of individual security rather than national security.[12] The Working Group of the Freedom Online Coalition[13] – a partnership of 30 governments working to advance Internet freedom – has codified a similar perspective, defining cybersecurity as protecting information and the Internet infrastructure for the sake of enhancing the security of individuals, both online and offline.[14]

There are also differences in the ways various players understand concepts such as critical information infrastructure (CII), cyber-weapons, and cyberterrorism. While there are some attempts to collect different terminology used in policy documents around the world, and explain the context in which they are used – such as the Global Cyber Definitions Database[15] which contains over 400 political definitions of cybersecurity and information security, and the list of cyber definitions provided by the CCD COE,[16] or the *Critical Terminology Foundation* by the EastWest Institute.[17] There is also a need to develop Cybersecurity Glossary that could help diplomats and practitioners to understand semantic coverage of terminology used by different actors involved in cybersecurity activities.

These terminological differences are of fundamental importance for international co-operation and negotiation about cyberspace.[18] Lack of common language increases the risk of miscommunication that could, at best, confuse messages and, at worst, lead towards conflict escalation.

[8] White House (no date) Foreign Policy: Cybersecurity. Available at https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

[9] Infosecurity (2011) Russian, US Experts Develop Common Definitions of Cybersecurity Terms. Available at http://www.infosecurity-magazine.com/view/17681/russian-us-experts-develop-common-definitions-of-cybersecurity-terms/

[10] Korzak E (2015) The next level for Russia-China cyberspace cooperation? Net Politics blog, Council on Foreign Relations, 20 August. Available at http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/

[11] Brown AD (2011) Challenges from the Cyber Domain: Cyber Security and Human Rights. Available at http://www.slideshare.net/adb-01/challenges-from-the-cyber-domain-cyber-security-and-human-rights

[12] Puddephatt A and Kasper L (2015) Cybersecurity is the new battleground for human rights. OpenDemocracy, 18 November. Available at https://www.opendemocracy.net/wfd/andrew-puddephatt-lea-kaspar/cybersecurity-is-new-battleground-for-human-rights

[13] More information about the FOC Working Group 1 is available at https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/

[14] Freedom Online Coalition (2015) Recommendations for Human Rights Based Approaches to Cybersecurity. Available at https://www.freedomonlinecoalition.com/wp-content/uploads/2015/11/FOC-WG1-Recommendations-discussion-draft-IGF-2015-new.pdf

[15] The report Compilation of Existing Cybersecurity and Information Security Related Definitions and the online database of definitions are available at http://cyberdefinitions.newamerica.org/

[16] Cyber definitions of the CCD COE are available at https://ccdcoe.org/cyber-definitions.html

[17] Rauscher K F and Yaschenko V (2011) Critical Terminology Foundations. EastWest Institute and the Information Security Institute. Available at: https://www.east-west.ngo/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations

[18] Giles K and Hagestad II W (2013) Divided by a Common Language: Cyber Definitions in Chinese, Russian and English, in Proceedings of the 5th International Conference on Cyber Conflict, Podins K et al. [eds], Tallinn: NATO CCD COE Publications. Available at: https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf

2 Diplomatic initiatives

2.1 Major initiatives and instruments

In response to increasing cyber-armament, diplomatic initiatives have emerged attempting to codify state behaviour in cyberspace and encourage co-operation to reduce the risk of conflicts. On an international level, the UN has established dialogue among a number of states through the GGE,[19] while several regional organisations – such as the OSCE in Europe, ASEAN Regional Forum, and the OAS – have also set up their own mechanisms for discussing ways to reduce risks from the misuse of ICT. The SCO has proposed the International Code of Conduct for Information Security. The European Union and the African Union are addressing the broader context of cybersecurity through their policy documents, while NATO, the OECD, and the G20 are focusing on particular aspects related to their agenda. Interestingly, even the private sector – namely, Microsoft – has joined in with proposed international cybersecurity norms for states and industry.

The two common political instruments shaped in these initiatives are voluntary norms of state behaviour in cyberspace and CBMs to reduce conflict; specific aspects of capacity building are also suggested. Norms are understood in the broader context of regime theory as 'standards of behaviour defined in terms of rights and obligations'.[20] The UN GGE report[21] states that 'norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States.' CBMs, on the other hand, are 'planned procedures to prevent hostilities, to avert escalation, to reduce military tension, and to build mutual trust between countries', according to the UN Office for Disarmament Affairs (UNODA).[22] CBMs can 'increase interstate co-operation, transparency, predictability and stability', and 'enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs'.[23] Capacity building is observed as needed assistance, especially to developing countries, to improve 'the capacity of states for co-operation and collective action'; importantly, it is recognised that capacity building 'involves more than a transfer of knowledge and skills from developed to developing State, as all States can learn from each other about the threats that they face and effective responses to those threats'.[24]

2.1.1 UN GGE[25]

Information security has been on the UN agenda since 1998[26] when the Russian Federation introduced a draft resolution in the First Committee of the UN General Assembly (UNGA), which was adopted without a vote.[27] While UNGA resolutions remain largely non-binding, they are the only ones voted on by all members of the UN. In 2004, the first GGE on Developments in the Field of Information and Telecommunications in the Context of International Security was established as a UN-mandated working group in the field of information security looking to 'examine the existing and potential threats from the cyber-sphere and possible co-operative measures to address them.[28] Four working groups have been established since 2004; the fifth was established for the period 2016/2017. The UN GGE can be credited with two major achievements: outlining the global cybersecurity agenda, and introducing the principle that international law applies to the digital space.

The GGE's composition is based on equitable geographical distribution. The five permanent members of the Security Council traditionally have a seat on all GGEs, and the remaining seats are allocated by UN regional grouping. States often send an official request for a seat on a GGE of particular interest to them, and might even lobby at the highest levels of the Secretariat for a place at the table. The Office of the High Representative for Disarmament has the task of proposing the Group's composition to the Secretary-General, considering not only geographical and political balance, but a demonstrated interest in the topic, the number of times that a country has served on other GGEs, whether they are currently serving on a different GGE, etc. Occasionally a government might decline to participate in a GGE if it believes it lacks the personnel or expertise necessary for the work. The first three groups consisted of experts from 15 countries, the fourth was extended to 20 members, while the fifth group has 25 members. Figure 3 shows a map of countries whose experts participated in the GGE, and those that chaired the group.

Reports are the main outcome of the UN GGE's work. Although the reports are not legally binding, they carry significant influence in the field of global cybersecurity. The 2010 report[29] included recommendations for further dialogue among states to reduce the risk and protect critical national and international infrastructure; called for confidence-building, stability, and risk-reduction measures; suggested voluntary information exchanges on national

[19] UNODA (United Nations Office for Disarmament Affairs) (no date) GGE Information Security. Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://www.un.org/disarmament/topics/informationsecurity/

[20] Krasner S (1982) Structural causes and regime consequences: Regimes as intervening variables. International Regimes 36(2), pp. 185–205.

[21] UN GGE (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[22] UNODA (no date) Military confidence-building. UNODA website. Available at https://www.un.org/disarmament/cbms/

[23] OSCE (2012) Permanent Council Decision No.1106. Available at http://www.osce.org/pc/109168?download=true

[24] Ibid. 52

[25] The Geneva Internet Platform Digital Watch has a dedicated page which provides detailed information about the GGE's operational modality, milestones, and related documents, and follows GGE developments. Available at http://digitalwatch.giplatform.org/processes/ungge

[26] For an analysis of relevant resolutions, refer to Radu R (2013), Negotiating Meanings for Security in the Cyberspace. Info, 15(6) pp. 32–41. Available at http://www.emeraldinsight.com/doi/abs/10.1108/info-04-2013-0018

[27] A/RES/53/70 is available at http://undocs.org/A/RES/53/70; refer also to UNODA's dedicated webpage, available at http://www.un.org/disarmament/topics/informationsecurity/

[28] UNODA (2013) Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security. Available at http://unoda-web.s3.amazonaws.com/wpcontent/uploads/2013/06/Information_Security_Fact_Sheet.pdf

[29] A/65/201 is available at http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201

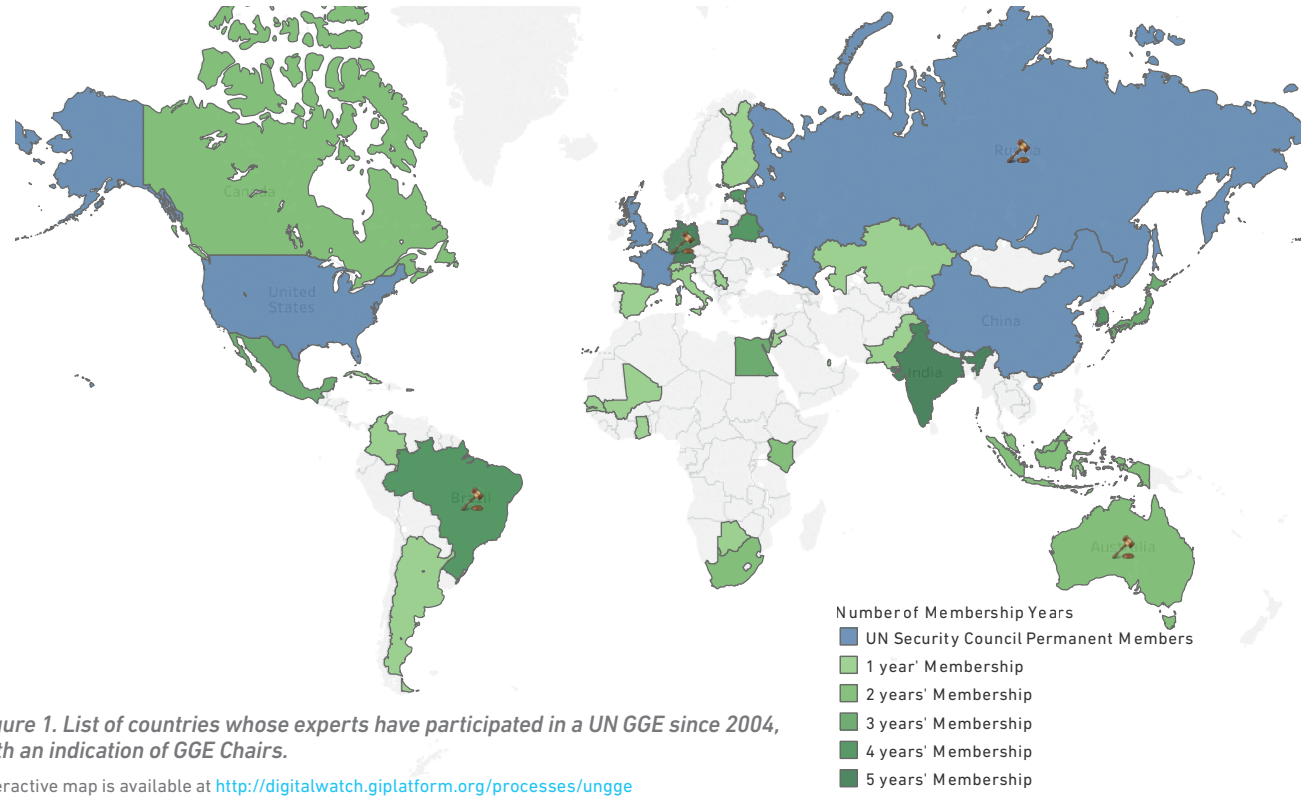


Figure 1. List of countries whose experts have participated in a UN GGE since 2004, with an indication of GGE Chairs.

Interactive map is available at http://digitalwatch.giplatform.org/processes/ungge

legislation and strategies; proposed capacity-building measures; and suggested the elaboration of common terms and definitions related to information security.

The 2013 GGE report clearly outlined growing trends of cyber-militarisation in a number of countries, and confirmed the overall agreement of participating states that 'international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[30,31] The report included the norms, rules, and principles on the responsible behaviour of states; a reference that state sovereignty applies to the digital field; and the principle that states must meet their international obligations regarding internationally wrongful acts in cyberspace attributable to them. The GGE report of 2015[32] was a breakthrough: 20 countries, including the USA, China, Russia, France, the UK, and Germany, specified the normative framework for state behaviour and agreed on a set of norms and CBMs, including co-operation in combating cybercrime and avoiding the targeting of critical infrastructure (including national Computer Emergency Response Teams (CERTs)), in the case of possible conflicts in cyberspace.

2.1.2 Major regional cybersecurity initiatives related to norms and CBMs

OSCE

On 26 April 2012, the Permanent Council of the OSCE, the largest regional security organisation in the world with 57 participating states from Europe, Central Asia, and North America, adopted Decision No. 1039[33] on CBMs to reduce the risk of conflict stemming from the use of ICT. The subsequent decision, no. 1106[34] from December 2013 outlines 11, mostly concrete, measures that participating states are invited to follow, on a voluntary basis. Measures include sharing national views on threats and best practices, co-operating with competent national bodies, consulting to reduce risks of misperception and possible tension or conflict, building up national legislation to allow information sharing, and sharing and discussing national terminology related to cybersecurity.

In March 2016, the OSCE adopted Decision No. 1201[35] which presents a second set of CBMs. The key progress that the five new CBMs bring is in a detailed measure that encourages co-operation in CI protection, and another that encourages responsible reporting on vulnerabilities in ICT systems and co-operation to address them. In addition, the new CBMs encourage public-private partnerships and the involvement of the private sector, academia, centres of excellence, and civil society in cybersecurity measures, and recognise the UN GGE's efforts while suggesting that the OSCE CBMs complement them and avoid duplication.

ASEAN Regional Forum

The ASEAN Regional Forum (ARF) came up with *Work Plan on Security of and in the Use of Information and Communications Technologies*[36] in 2015, which came as result

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

[31] A/68/98* is available at http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

[32] A/70/174 is available at http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[33] OSCE Permanent Council Decision No. 1039. Available at http://www.osce.org/pc/90169

[34] OSCE Permanent Council Decision No.1106. Available at http://www.osce.org/pc/109168?download=true

[35] OSCE Permanent Council Decision No.1201. Available at http://www.osce.org/pc/227281?download=true

[36] ASEAN Regional Forum. 'Work Plan on Security of and in the Use of Information and Communications Technologies'. Available at http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf

of the 2012 statement by the ARF Ministers of Foreign Affairs (MFAs).[37] The ARF invites states to share information among designated contact points (without duplicating CERT networks); to conduct surveys on lessons learned in dealing with threats; to organise discussion exercises related to preventing cyber-incidents; and to work out channels for online information sharing on threats to critical infrastructure, and modalities for real time information sharing. Further, it invites co-operation and information sharing on combating criminal and terrorist use of ICT, and discussing terminology to promote understanding of different national practices. Importantly, the ARF also invites capacity building and research and analysis activities related to ICT security.

OAS

The OAS has used a somewhat different approach by adopting its Comprehensive Inter-American Cybersecurity Strategy[38] in 2004, looking at building a cybersecurity culture that would prevent misuse and encourage trust. The strategy suggests developing a regional warning network to alert and inform about incidents, building a shared secure infrastructure for managing sensitive Computer Security Incident Response Team (CSIRT) communications with the private sector and other stakeholders, setting up technical cybersecurity standards, and increasing legal capacities for combating cyber-crime. The strategy specifically invites co-operation of the public and private sectors and academia in protecting CI and the critical ICT infrastructure. It advocates the use of public-private partnership in awareness-raising and educational programmes, engagement of all the actors in development of strategic and implementation plans on national levels, and the initiating of relevant capacity-building programmes.

The OAS Inter-American Committee Against Terrorism (CICTE) has adopted in 2012 a Declaration on *Strengthening Cyber-Security in the Americas,*[39] which reminds member states of the commitment to implement the 2004 Strategy, invites for establishing national CSIRTs and developing national strategies that engage all relevant stakeholders, and particularly focuses on protection of critical infrastructure through information sharing, public-private partnerships and capacity building. In 2016, CICTE has adopted a Declaration on *Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in the Americas,*[40] which further invites member states to respect human rights in the use of cyberspace, strengthen co-operation among CSIRTs as well as among law enforcement institutions, develop protocols for communication among member states in case of incidents whose effects surpass national borders as well as procedures for mutual assistance when responding to incidents, commit to creating confidence-building measures that strengthen international peace and security, and assist CICTE to deliver capacity building support to member states. The OAS resolutions also outline general confidence- and security-building measures, not addressing cybersecurity directly.[41]

2.1.3 Other frameworks and initiatives

SCO

At the end of 2011, the countries of the SCO proposed an International Code of Conduct for Information Security[42] to the UN. Among other provisions, the draft highlighted respect for sovereignty and territorial integrity, and called on states to co-operate in combating cybercrime and terrorist use of ICT, not to use ICT for hostile activities and aggression, nor to proliferate information weapons. The draft proposal, however, envisaged wider coverage than just cyber-conflict, including Internet governance issues, surveillance, and content policy; for instance, it invites the establishment of a democratic and multilateral internet management system.[43] In 2015, the SCO re-introduced an updated version of the proposal,[44] which, among few changes, removed the invitation not to proliferate information weapons, and suggested that 'the rights of an individual in the offline environment must also be protected in the online environment'.

European Union

The EU Cybersecurity Strategy[45] of 2013, entitled *An Open, Safe, and Secure Cyberspace*, represents the EU's vision on how best to prevent and respond to cyber disruptions and attacks in terms of five priority areas:

- Achieving cyber resilience.
- Drastically reducing cybercrime.
- Developing a cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP).
- Developing industrial and technological resources for cybersecurity.
- Establishing a coherent international cyberspace policy for the EU and promoting core EU values.

The EU *Directive on Network and Information Security*[46] (known as the NIS Directive), adopted in July 2016, aims at strengthening overall cybersecurity in the EU. It requires each member state to adopt a national cybersecurity strategy, to establish a CSIRT, and to appoint a competent national authority for network and information security (NIS) to act as the main point of contact on the issue with other countries. The directive also sets up a cross-EU co-operation group for strategic co-operation and a CSIRT Network for operational co-operation, among other provisions. The directive defines several categories of 'op-

[37] ASEAN Regional Forum. Statement by the Ministers of Foreign Affairs on Co-operation in Ensuring Cyber Security. Available at http://www.mofa.go.jp/files/000016403.pdf

[38] OAS. Comprehensive Inter-American Cybersecurity Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. Available at http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

[39] OAS Inter-American Committee Against Terrorism Declaration 'Strengthening Cyber-Security in the Americas'. Available at http://www.state.gov/p/wha/rls/221498.htm

[40] OAS Inter-American Committee Against Terrorism Declaration 'Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in the Americas'. Available at http://www.state.gov/p/wha/rls/259346.htm

[41] The list of confidence- and security-building measures by the OAS is available at: http://www.oas.org/csh/english/csbmlist.asp

[42] SCO (2011) SCO proposal for the International code of conduct for information security. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/66/359

[43] CCD COE (2015) An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New? Available at https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

[44] SCO (2015) SCO proposal for the International code of conduct for information security. Available at http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723

[45] European Commission (2013) EU Cybersecurity Strategy. Available at https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[46] European Commission (2015) EU Network and Information Security Directive. Available at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

erators of essential services', which are required to take appropriate security measures and notify the relevant national authority of any serious incidents. This includes operators in the following sectors: energy, transport, banking, financial market infrastructures, health, water, and digital infrastructure (including Internet exchange points, domain name system service providers, and top-level domain name registries).

African Union

The African Union's *Convention on Cyber Security and Personal Data Protection*,[47] adopted in 2014, provides a legal framework for promoting cybersecurity, combating cybercrime, conducting electronic commerce, and protecting personal data. Its impact on the national legal frameworks, however, remains limited so far, as only eight countries had signed it by June 2016.

OECD

The OECD mainly focuses on the issues related to Internet economy, e-government, and privacy, while its cybersecurity-related activities are mostly linked to the security of electronic transactions, protection of CII and building up cybersecurity strategies. The OECD *Recommendation of the Council on the Protection of Critical Information Infrastructures*[48] of 2008 outlines several recommendations for states, including adopting national policies and identifying authorities in charge, co-operating with private sector owners and operators of CII, conducting regular risk assessment. It also provides recommendations on protecting CII across borders, including sharing knowledge and experience bilaterally and with private CII operators.

NATO

Following the 2007 cyber-attacks on Estonia, NATO defence ministers agreed on immediate action in the event of cyber-attack and in 2008 they established the CCD COE in Estonia. In 2015, NATO took an official position that 'cyber-attacks can potentially trigger an Article 5 response' (which holds that an attack on one nation is an attack on all), as stated by NATO Secretary General Jens Stoltenberg.[49] In 2016, NATO officially enlisted cyberspace as the fifth domain of warfare and made a Cyber Defence Pledge[50] recognising the need to protect NATO member states against cyber-attacks.[51]

G20

The group of 20 major economies has put cyber-espionage high on its agenda: in November 2015, the G20 agreed that 'that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors' (article 26).[52] The 2016 G20 meeting in Hangzhou, China, however, produced a somewhat different message: The Communiqué[53] resulting from that meeting did not deal with cybersecurity beyond mentioning it.[54]

Wassenaar

Diplomatic processes related to disarmament also increasingly consider cyber aspects. The list of dual-use goods and technologies of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,[55] a multilateral export control regime gathering over 40 countries around the world, was expanded in 2014 to include intrusion software (malware and intrusion exploits, including 'zero-day') and surveillance products.[56] China raised the SCO's proposal on the International Code of Conduct for Information Security at the Conference on Disarmament (CD); however, internal challenges may prevent the CD from comprehensively adding cyber issues to its agenda at the time.[57]

Microsoft

In addition to international organisations, a novelty in the field of international cybersecurity came from the private sector: Microsoft has proposed International Cybersecurity Norms for reducing conflict in an Internet-dependent world.[58] The initiative came as result of the understanding in the private sector that the eventual use of ICT in international conflicts would inevitably impact the global economy, including the online industry, and that the weapons used would be based on exploiting intrinsic vulnerabilities in complex software and hardware solutions, which would additionally decrease trust in the online environment. The proposed norms call on states not to require ICT companies to insert backdoors into products; to report identified product vulnerabilities to vendors rather than stockpile, buy, sell or exploit them; to restrain from developing cyber-weapons and ensure that those developed ones are limited, precise, and not reusable; to commit to non-proliferation activities; to limit their engagement in cyber offensive operations to avoid creating mass events; and to assist the private sector in detecting, containing, responding to, and recovering from cyber-incidents. Building on these proposed norms, and realising the responsibility of the private sector as well, in 2016 Microsoft also suggested a set of norms for the global ICT industry.[59]

[47] African Union (2014) African Union Convention on Cyber Security and Personal Data Protection. Available at http://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[48] OECD (2008) Recommendation of the Council on the Protection of Critical Information Infrastructures. Available at https://www.oecd.org/sti/40825404.pdf

[49] NATO (2015) Keynote speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar. Available at http://www.nato.int/cps/en/natohq/opinions_118435.htm

[50] NATO (2016) Cyber Defence Pledge. Available at http://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en

[51] CCD COE (2016) NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. Available at https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html

[52] G20 (2015) G20 Leaders' Communiqué. Antalya Summit, 15-16 November 2015. Available at http://pm.gc.ca/eng/news/2015/11/16/g20-leaders-communique

[53] G20 (2016) The G20 Leaders' Communiqué Hangzhou Summit. Available at http://www.g20.org/English/Dynamic/201609/t20160906_3396.html

[54] Teleanu S (2016) Digital policy issues emphasised at the G20 Leaders' Summit. DiploFoundation blog. Available at https://www.diplomacy.edu/blog/digital-policy-issues-emphasised-g20-leaders%e2%80%99-summit

[55] Wassenaar (2015) List of dual-use goods and technologies of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Available at http://www.wassenaar.org/wp-content/uploads/2015/08/WA-LIST-15-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

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

[57] Grigsby A (2015) The UN GGE on Cybersecurity: What is the UN's role? Council on Foreign Relations Blog, 15 April. Available at http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/

[58] Microsoft (2015) International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World. Available at http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf

[59] Microsoft (2016) From Articulation to Implementation: Enabling progress on cybersecurity norms. Available at https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf

2.2 Bilateral cyber-relations

2.2.1 Bilateral cyber-dialogues and agreements

With the increasing frequency and intensity of cyber-attacks and their geopolitical and economic consequences, many countries are turning to bilateral relations concerning cyberspace. Relations vary from bilateral meetings to strategic partnerships (such as between Canada and Israel), from continuous dialogue (such as the EU-Japan cyber-dialogues) to statements and communiqués (such as the joint statement by the Prime Ministers of Sweden and India, or a joint declaration of Czech Republic and Israel), from Memorandums of Understanding (such as between the UK and Singapore) to bilateral agreements (such as between Brazil and Russia or between India and Russia).

Thematic coverage of bilateral arrangements varies from specific coverage such as co-operation in combating cybercrime and terrorist use of the ICT, cyber-defence, and non-aggression by information weapons, to broader coverage of cybersecurity co-operation (such as between India and Malaysia) or cyber-policy issues (such as between Japan and Australia) – often including privacy and data protection as well (such as between Brazil and the USA). Cybersecurity is often also part of co-operation agreements in the field of ICT, the information society, or Internet governance (such as the trilateral India-China-Russia meeting of Foreign Ministers).

A non-exhaustive mapping of bilateral cyber-relations, graphically represented in Figure 4, accounts for over 100 already established relations in the field of cybersecurity, cyber policy, ICT, and the information society. It is expected that the list will grow further as cyber comes to the forefront of the diplomatic agenda, and as capacities and awareness also increase in developing countries.

2.2.2 Bilateral cyber-relations among major economies

The lead economies are also the leaders in establishing mutual relationships on cyber issues. Some of the key bilateral arrangements and dialogues include:

- **EU with third countries:** The EU cyber-dialogues with China, India, Japan, South Korea, and the USA had started by 2015,[60] while the dialogue with Brazil is pending. Most formal negotiations are accompanied by informal dialogue with other experts and stakeholders in these countries, such as the Sino-European Cyber Dialogue.
- **USA and China:** In September 2015, the presidents of the USA and China met to discuss, among other issues, increasing concerns about cyber-incidents.[61] They agreed not to knowingly support cyber-espionage against the corporate sector.[62]
- **USA and Russia:** In 2013, the USA and Russia engaged in dialogue to reduce the danger from cyber-threats.[63] The agreement envisaged establishing a direct 'cyber-hotline' between the White House and

[60] European Parliament (2016) Cyber diplomacy: EU dialogue with third countries. Briefing. Available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf

[61] Holland S (2013) Obama, China's Xi discuss cyber security dispute in phone call. Reuters, 14 March. Available at http://www.reuters.com/article/2013/03/14/us-usa-china-obama-call-idUSBRE92D11G20130314

[62] Spetalnick M and Martina M (2015) Obama announces 'understanding' with China's Xi on cyber theft but remains wary. Reuters, 26 September. Available at http://www.reuters.com/article/2015/09/26/us-usa-china-idUSKCN0RO2HQ20150926#QCl52gO5xlJVWVja.97

[63] The White House (2013) FACT SHEET: US-Russian Cooperation on Information and Communications Technology Security. Available at https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

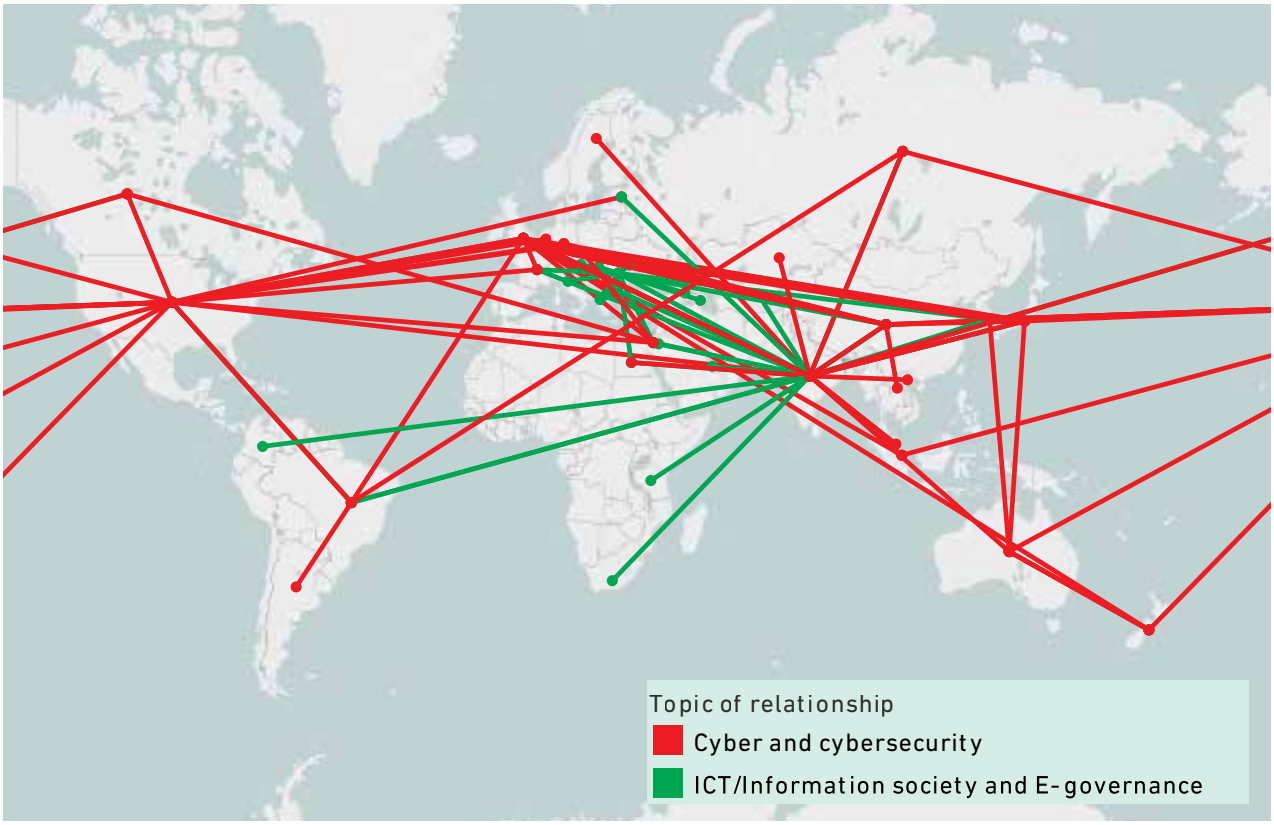


Figure 2. Map of bilateral cyber-agreements.
DiploFoundation; interactive map is available at https://public.tableau.com/profile/publish/cyberagreements/Dashboard1#!/publish-confirm

the Kremlin, an operational link between CERTs, and a bilateral working group to extend co-operation related to national security concerns. The co-operation, however, was frozen in 2014 due to tensions over the situation in Ukraine. Meetings between US and Russian cybersecurity officials in Geneva in April 2016 focused on the work of the UN GGE and the OSCE CBMs.[64]

- **Russia and China:** The presidents of Russia and China concluded a cyber-agreement according to which both sides will refrain from carrying out cyber-attacks against each other, will support each other's cyber-sovereignty, and will jointly respond to technologies that may 'destabilize the internal political and socio-economic atmosphere'.[65]
- **USA and India:** The Indian prime minister and the US president agreed to finalise a joint Framework for the US-India Cyber Relationship focusing on cybersecurity.[66] The framework should include developing co-operation among law enforcement agencies and CERTs, strengthening the security of CI, restraining from cyber-espionage, combating various cyber-attacks by state and non-state actors, and investing in research and development of cybersecurity products. The agreement supports the multistakeholder model of Internet governance, which moves India closer to the position of the USA and its allies and further from the position of China and Russia.
- **India and Russia:** On the margins of the October 2016 BRICS Summit, India and Russia signed a formal bilateral cybersecurity agreement covering cybercrime co-operation but also matters of combating cyber-terrorism and protecting the critical infrastructure, as well as defence and national security co-operation.[67] This means that India is the only major power to have established formal cybersecurity frameworks with both Russia and the USA.
- **China and Germany:** Chinese and German officials have started working on a cybersecurity no-spy agreement similar to the one between China and the USA, as was confirmed after the visit of German Chancellor Merkel to Beijing.[68]
- **China and Canada:** Canada and China have started a series of negotiations on a possible bilateral agreement on cybersecurity, which may be similar to the China-US agreement, focusing particularly on preventing economic cyber-espionage to protect the intellectual property of the Canadian industry.[69]

While these relationships vary in form and content, it is evident that there is a growing need for enhancing the co-operation, to prevent misunderstanding and possible conflicting situations. These bilateral relations, however, should not replace or reduce the importance of international and regional processes; on the contrary, the two should feed into and fuel each other.

[64] Pawlak P (2016) Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: International Cyber Norms: Legal, Policy & Industry Perspectives, Osula AM and Rõigas H (eds), NATO CCD COE Publications, Tallinn 2016, pp.129–153. Available at https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf

[65] Razumovskaya O (2015) Russia and China pledge not to hack each other. The Wall Street Journal, 8 May. Available at http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/

[66] The White House (2016) Joint Statement: The United States and India: Enduring Global Partners in the 21st Century. Available at https://www.whitehouse.gov/the-press-office/2016/06/07/joint-statement-united-states-and-india-enduring-global-partners-21st

[67] Sukumar AM (2016) India and Russia sign cyber agreement, pushing the frontier for strategic cooperation. ORF Digital Frontiers. Available at http://www.orfonline.org/expert-speaks/india-and-russia-cyber-agreement/

[68] Nicola S (2015) China working to halt commercial cyberwar in deal with Germany. Bloomberg, 29 October. Available at http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany

[69] Freeze C (2016) Canada, China to discuss accord on cybersecurity. The Globe and Mail. Available at http://www.theglobeandmail.com/news/national/canada-china-to-discuss-accord-on-cybersecurity/article32068707/

3 Comparison of major instruments

3.1 Norms and CBMs

The UN GGE reports lay out sets of cyber-norms as well as CBMs. The documents of the three dominant frameworks of regional organisations mentioned earlier – the OSCE, ARF, and the OAS – outline CBMs and measures that either overlap with or complement each other and with the UN GGE. Looking at the specific measures, it is evident that there is both the influence of GGE on regional measures, and the potential of regional measures to complement the GGE measures.[70]

One possible classification of norms and measures outlined by the GGE, OSCE, ARF, and OAS documents is according to their main role:

- Encouraging the exchange of information
- Appointing contact points
- Enhancing CERT/CSIRT co-operation
- Protecting CI and CII
- Combating cybercrime and terrorist use of ICT
- Reducing the risk of misperception
- Developing common terminology
- Developing norms of behaviour
- Facilitating ongoing dialogue
- Encouraging multistakeholder approach
- Implementing capacity building
- Encouraging research

Table 1 presents the coverage of each of the roles in particular documents. It is evident that the GGE is more comprehensive than any of the regional documents, as it mainly sets the trends followed by regional organisations.

A more detailed investigation of the main proposed measures in all the documents, however, reveals that there are particular regional measures that could stimulate follow-up by the GGE. What follows is an overview of the main measures proposed by the various documents, presented in a descriptive manner.

Encouraging the exchange of information

States are encouraged to share information among themselves, and in particular:

- National views about the role of ICT in conflict (GGE) and national and transnational aspects of threats (OSCE)
- Information about national frameworks, such as laws, strategies, policies, best practices (GGE) including successful public-private partnerships (OSCE)
- Experiences and lessons learned (OSCE) in dealing with threats, and creation of regional database of potential threats and possible remedies, in co-operation with working with CERTs (ARF)
- Plans to develop an online resource for sharing cybersecurity information (OAS)
- Information about incidents, threats, and hidden functions (GGE), measures to protect the critical infrastructure and respond to incidents (OAS), facilitation of responsible disclosure and reporting on vulnerabilities, and sharing of information on remedies – including with the ICT industry – through authorised and protected communication channels such as authorised contact points (OSCE and GGE)

[70] A particularly rich analysis and comparison of norms and CBMs in the UN and various regional frameworks is provided in Pawlak P (2016) Confidence-Building Measures in Cyberspace: Current Debates and Trends. In: International Cyber Norms: Legal, Policy & Industry Perspectives, Osula AM and Rõigas H (eds), NATO CCD COE Publications, Tallinn, pp.129–153. Available at https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf

	GGE	OSCE	ARF	OAS
Exchange of information	♦	♦	♦	♦
Contact points	♦	♦	♦	
CERT/CSIRT	♦			♦
CI and CII	♦	♦	♦	♦
Cybercrime and terrorism	♦	♦	♦	♦
Reducing the risk of misperception	♦	♦	♦	♦
Common terminology	♦	♦	♦	
Norms	♦		♦	
Facilitating ongoing dialogue	♦	♦		♦
Multistakeholder approach	♦	♦		♦
Capacity building	♦	♦	♦	♦
Research	♦		♦	

Table 1. Overview of the main roles covered by UN GGE, OSCE, ARF, and OAS documents.

In this regard, the GGE brings advanced measures, such as sharing information about hidden functions in software and hardware (also known as backdoors). The OSCE, however, puts greater emphasis on the role of other stakeholders and public-private partnerships in building national frameworks, which may be a valuable message for the GGE. ARF suggests creating a regional database of potential threats and remedies – a proposal which may be followed by other regions or also at international level, bearing in mind the global nature of cyber-threats.

Appointing contact points

States are encouraged to set-up mutual points of contact, particularly:

- Nominating a national contact point and provide contact data of existing national structures (such as CERTs), updating contacts annually, and notifying about changes (OSCE and GGE)
- Sharing information among appointed contact points, and establishing a contact directory/database – without duplicating CERT networks (ARF and GGE)

In this regard, the OAS could consider the value of clearly suggesting member states to nominate contact points, and maintaining the database.

Enhancing CERT/CSIRT co-operation

States are encouraged to enhance the role of CERTs/CSIRTs, particularly through:

- Establishing CERTs (GGE and OAS) including for the protection of CI (GGE), and facilitating co-operation among CERTs (GGE and OAS), such as exchanging information on known vulnerabilities, attack patterns, and best practices for mitigating the threats; coordinating responses; organising exercises; supporting each other in handling incidents; and facilitating regional co-operation (GGE)
- Not conducting or knowingly supporting activities to harm CERTs of other states, nor using CERTs to engage in malicious international activities (GGE)

In this regard, the GGE has advanced with particular norms of behaviour, but has also recognised the particular importance of CERTs. Neither OSCE nor ARF documents clearly outline the need for and the role of CERTs, which may be a necessary step to undertake in future.

Protecting critical infrastructure and critical information infrastructure

States are advised to put additional emphasis on protecting CI and CII, in particular through:

- Exchanging information about categories of national CI (GGE) and policy and operational measures to protect them (GGE, OAS)
- Creating a repository of laws and policies on protecting CII and classification of incidents (GGE)
- Protecting national and cross-border CII and CI (GGE, ARF, and OSCE) through collaboration between legally authorised authorities for CI (OSCE), including sharing information on threats (GGE, ARF, and OSCE); developing shared response like crisis management; classifying ICT incidents in terms of scale and infrastructure; sharing national views on what is CI (OSCE); conducting consultations; implementing technical, legal, and diplomatic mechanisms; and co-operating in addressing incidents against CI and CII (GGE)
- Facilitating cross-border co-operation to address basic infrastructure vulnerabilities that transcend national borders (OAS);
- Providing channels for online information sharing on threats to CI, and modalities for real time information sharing, together with CERTs (ARF)
- Not conducting or knowingly supporting activity that intentionally damages CI or otherwise impairs the use and operation of CI to provide service to the public (GGE)
- Responding to appropriate requests for assistance by another state whose CI is subject to malicious ICT acts, mitigating malicious acts against CI of another state emanating from its territory, taking into account due regard for sovereignty (GGE)
- Ensuring the co-operation of the public and private sectors and academia in protecting CI and CII, and organising capacity building programmes (OAS)
- Developing a global culture of cybersecurity (GGE)

While all the documents clearly recognise high importance of protecting CI and CII, the GGE has the most advanced measures – including the norms related to not conducting attacks against CI. The OSCE, however, provides some useful complementary details that the GGE could consider. The OAS, on the other hand, adds important emphasis on the greater involvement of the private and academic sectors in protecting CI, and directly invites much-needed capacity building measures – measures that other forums could take into consideration.

Combating cybercrime and terrorist use of ICT

States are invited to contribute to combating criminal and terrorist use of ICT, in particular through:

- Harmonised (GGE) legislation that facilitates (OSCE) mutual assistance (GGE), information sharing and co-operation of legal practitioners (ARF), prosecutorial agencies (GGE), competent national bodies and law enforcement authorities to counter crime and terrorism (ARF, OSCE, and GGE) through technical, legal and diplomatic mechanisms (GGE)
- Joint task force between countries (ARF)
- Laws to protect information systems, prevent illegal activity and punish cybercrime (OAS)
- Establishing specialised units within law enforcement authorities and enhancing their regional co-operation (OAS).

Despite the evident awareness of the importance of co-operation against cybercrime and terrorist use of ICT, such co-operation is in practice still way beyond what might be needed. In this regard, all the documents will likely contribute to more efficient co-operation. It is of concern, however, that no measure calls for co-operation with the Internet industry: this is a much-needed component of successful digital forensics and law enforcement regarding criminal acts in cyberspace, and both the GGE and regional frameworks might consider addressing it.

Reducing the risk of misperception

States are encouraged to strengthen co-operation that could reduce the risk of misperception and escalation of tensions, in particular through:

- Consulting to reduce the risks of misperception and political or military tension or conflict (OSCE)
- Considering, in case of incidents, larger context of the event, the challenges of attribution in cyber, and the nature and extent of consequences (GGE)
- Introducing measures for rapid communication at policy levels of authority, to discuss on national security level (OSCE)
- Establishing senior point of contact between countries for real time communications on incidents of regional security relevance (ARF)
- Developing activities for experts and officials to support facilitation of authorised and protected communication channels (OSCE)
- Clarifying technical, legal, and diplomatic mechanisms to address requests from other states (OSCE)
- Creating frameworks and protocols for co-operation in case of incidents whose effects surpass national borders, and procedures for mutual assistance when responding to incidents (OAS)
- Taking into account that indication that activity was launched or originates from the territory or the infrastructure of state may be insufficient to attribute to activity of the state, and, in case accusations are made, substantiate them (GGE)

The UN GGE outlines specific norms regarding reducing the risk of escalation of tensions. Nevertheless, the OSCE and the ARF frameworks provide operational measures which may directly serve to facilitate communication in a time of increased tensions – measures that the GGE may additionally focus on in future. The OAS has suggested few co-operation measures within its 2016 Declaration, yet it may consider further developing them in future upgrades of its co-operation framework.

Developing common terminology

States are encouraged to invest in agreeing on common terminology used for communications, including through:

- Discussing terminology to promote understanding of different national practices and usage (ARF)
- Elaborating common terms and definitions (GGE)
- Providing a list of national terminology with explanations or definitions, and, in the longer term, producing a consensus glossary (OSCE)

All the forums, except for the OAS, recognise the need to work on better understanding the terminology used by various parties. The GGE, even though it initially mentioned the need to elaborate on common terms and definitions in its report of 2010, has not worked out this initiative in subsequent reports. The OSCE seems to have gone furthest with its measure, yet there is an evident need for all the fora to invest more into this endeavour.

Developing norms of behaviour

States are invited to work on defining norms of state behaviour in cyberspace. In particular, states should:

- Discuss rules, norms, and principles of responsible behaviour and the role of cultural diversity in the use of ICTs (ARF)
- Co-operate in developing and applying measures to increase stability and prevent harmful ICT practices (GGE)
- Co-operate on implementation of norms, including with private sector and civil society (GGE)

In addition, the GGE reports outline several specific norms, most notably that:

- International law, and especially the Charter of the United Nations, is applicable to cyberspace.
- State sovereignty and jurisdiction over ICT infrastructure applies within own territory.
- States need to respect human rights and fundamental freedoms as stipulated in the Universal Declaration of Human Rights and other international documents.
- States should meet international obligations regarding internationally wrongful acts attributable to them.
- State must not use proxies to commit internationally wrongful acts using ICT, and should ensure that their territory is not used by non-state actors for unlawful use.
- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

Finally, the GGE outlines several specific aspects of the applicability of international law to cyberspace, related to sovereignty, settlement of disputes, respect for human rights, and established principles of international law, among others.

It is reasonable to expect that the GGE, as the working modality of the UN, will work more on developing particular norms of behaviour, while regional organisations will mainly focus on CBMs and merely invite further norms to be developed. Nevertheless, regional organisations can bring important inputs to development of norms at international level, such as ARF's call for discussing role of cultural diversity in the use of ICTs.

Facilitating ongoing dialogue

States are invited to support and facilitate ongoing dialogue through existing multilateral platforms, in particular through:

- Consultative frameworks (workshops, seminars) and inclusive dialogue (GGE)
- Mechanisms for bilateral, regional, subregional, and multilateral consultations (GGE)
- Exchanges (workshops, seminars, roundtables) to complement UN efforts and other forums, by inviting private sector, academia, centres of excellence, and civil society (OSCE)
- Discussion exercises on preventing incidents (ARF)
- Coordination among national organs, agencies, and entities, and through the OAS Permanent Council and the OAS Inter-American Committee Against Terrorism (OAS)
- Enhanced common understanding through regular dialogue within the UN (GGE)
- Regular dialogue through the OSCE Communication Network, with experts meeting at least three times a year (OSCE)

The OSCE initiative to involve private and civil sectors in ongoing communications is visible again, and may serve as an incentive to other forums – including the GGE – to incorporate similar elements. It is notable that various forums invite facilitated discussions through their own established mechanisms – the UN, the OSCE, and the OAS, in particular. While it is reasonable to expect that communi-

cations of regional concerns should be conducted through the regional framework, there may be a need for the GGE and the regional organisations to establish mechanisms to provide synchronisation between those forums and with the international level of the UN, to benefit from the regional knowledge and not to duplicate the efforts.

Encouraging multistakeholder approach

States are invited to consider greater involvement of other stakeholders within the dialogue, and in particular through:

- Involvement of the private sector and civil society, to play an appropriate role especially regarding securing the supply chain (GGE)
- Involvement of academia and centres of excellence in events (OSCE)
- National promotion of public-private partnerships and development of mechanisms for best practice for joint response to incidents (OSCE)
- Public-private partnerships for enhancing awareness and education about cybersecurity (OAS)
- Engagement of all relevant actors in strategy development and implementation, and adopting technical standards (OAS)
- Promoting public sector co-operation with the private sector and academia with regards to protection of the critical information infrastructure (OAS)
- Implementation of norms in co-operation with the private sector and civil society (GGE)

Even though the GGE is clearly inviting greater involvement of other stakeholders in implementing various measures and even norms, and emphasising its role for the security of supply chain, the OAS and the OSCE can be praised for their role as well. ARF, on the other hand, is missing explicit facilitation of co-operation with other stakeholders, which may change in future, primarily because of the GGE measures.

Implementing capacity building

Calls for enhanced capacity building efforts are made, in particular:

- Capacity building in developing countries (GGE)
- Capacity building for ICT security and combating criminal use (ARF)
- Awareness raising for non-technical personnel and policymakers on threats and methods to counter cyber-threats (ARF)
- Support by regional institution to states through regional awareness programme (OAS)
- Strengthening awareness programmes and campaigns, especially targeting vulnerable groups (OAS)
- Contribution of states to regional organisation to enable it to deliver capacity building (OAS)
- Utilisation of the OSCE as a platform to share information on capacity building (OSCE)

While all the forums recognise the importance of capacity building, the ARF framework provides some specific calls while the OAS emphasises the need for bi-directional support between regional organisations and member states. The OSCE, however, has merely a symbolic reference to capacity building, through inviting states to share information on various programmes through its platform; even though the OSCE does not gather least developed countries, the capacity building measures should not be disregarded (even for developed countries). Besides, the OSCE could be encouraged by other forums, and especially by the GGE, to work on capacity building for developing countries including non-members and to secure the broader environment. Ultimately, measures that could ensure joint efforts of various regional organisations and the UN in capacity building could bring about greater effects, and avoid duplication of efforts.

Encouraging research

States are invited to facilitate research in the field of ICT security, and in particular:

- Co-operation among research and academic institutions (GGE)
- Research and analysis on ICT security (ARF)

Other regions could also integrate specific measures about facilitating the research and the role of academia. This could lead to more evidence-based decisions and co-operation among states.

The comparison of these measures with other regional, multilateral, and private initiatives in the field provides additional possible improvements of current sets of CBMs and norms:

- **Intrusion:** While GGE norms address cyber-acts that result in 'damage' and 'impairment', none of the norms or CBMs address directly the attacks resulting in the intrusion or infiltration of systems. This is particularly relevant considering the increasing trends of cyber-espionage (as raised by the G20) and APT – hacks of and intrusions into the servers of industry, communication companies, financial sector, CI operators, and governmental institutions. These attacks remain under the threshold of current norms, yet increasingly impact global geopolitics and economy. Not addressing this type of attack renders current norms rather useless towards the most common and persistent types of attacks against states today.
- **Responsible disclosure:** While responsible disclosure of vulnerabilities by states is lightly touched on by the GGE reports and the OSCE CBMs, a more comprehensive approach might be needed to strengthen the resilience of the networks and prevent cyber-armament. The norms proposed by Microsoft are particularly relevant and useful in this regard, and might be considered in detail. In addition, initiatives like the Coordinated Vulnerability Disclosure run in partnership by states and institutions within the context of Global Forum on Cyber Expertise (GFCE) might be worth considering.[71]
- **Responsibility of the industry:** Similarly, the Microsoft norms also reflect the enhanced responsibility of the ICT/Internet industry for security of their products, which is becoming increasingly relevant considering the millions of connected devices of the Internet of Things that are shipped with insecurity-by-default. Future norms and CBMs could consider engaging the private sector in closer dialogue with states on ensuring the security-by-design concept instead.

[71] More information about the Coordinated Vulnerability Disclosure initiative within the GFCE is available at https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

3.2 Capacity building

All the discussed frameworks clearly recognise the importance of capacity building for effective implementation of norms and CBMs, and invite additional efforts in this regard. The proposed capacity building measures in the GGE, OSCE, ARF, and OAS documents, can be categorised in the following way:

Broad context topics

- Security of ICT in states (GGE)
- Cybersecurity and cyber-ethics (OAS)
- Benefits and responsibilities of using information networks (OAS)
- Potential negative consequences resulting from the misuse of networks (OAS)
- Awareness for non-technical personnel and policy-makers on threats (ARF)
- National legal, regulatory, and strategic frameworks (GGE)
- Awareness raising for Internet users about risks in cyberspace (OAS)

Co-operation to reduce risks of misperception

- Technical, legal, and diplomatic mechanisms to address requests (OSCE)
- Procedures for fast assistance in responding to incidents (GGE)

Combating crime and terrorism

- Combating criminal use of the Internet (ARF)
- Law enforcement capabilities and digital forensics (GGE) and evidence analysis (OAS)
- Co-operative measures against cybercrime and terrorism (GGE, OAS)
- Awareness programmes and campaigns targeting groups most vulnerable to cybercrime (OAS)
- Fighting terrorism and responding to terrorist incidents (OAS)

Incident response

- Incident response capabilities (GGE)
- CERT and CERT-to-CERT co-operation (GGE)
- How to report a cyber incident and to whom (OAS)

Technical assistance

- Co-operation of states with international organisations and private sector on technical assistance (GGE)
- Security and use of ICT (ARF)
- Technical skill and access to technologies for security (GGE)
- Safety and security best practices (OAS)
- Technical and practical information related to cybersecurity (OAS)

Critical (information/ICT) infrastructure

- CII and ICT infrastructure (GGE)
- Legal and administrative practices for cross-border co-operation to address CI vulnerabilities that transcend national borders (GGE)
- Strengthening of all critical components of the global supply chain and CII (OAS)
- Capacity for recovery of CII (OAS)

Sustainability of capacity building

- Developing strategies for sustainable capacity building (GGE)
- Prioritising ICT awareness and capacity building in national plans and budgets, and in development and assistance planning (GGE)
- Educating institutions and citizens, done in co-operation of UN, states, private sector, academia, and civil society organisations (GGE)
- Developing a regional approach to capacity building for specific cultural, geographical, political, economic, and social specificities (GGE)
- Conducting study and research by institutes and universities (GGE)
- Conducting e-learning, training, and awareness-raising to bridge the digital divide (GGE)
- Building multilateral and bilateral initiatives to improve effective mutual assistance to states (GGE)
- Encouraging states to assist regional organisations with contributions, to enable capacity building programmes (OAS)

Proposals cover a wide range of topics and target groups, clearly showing the need for a holistic approach. In addition, several suggestions reflect the sustainability of capacity building efforts, requiring a comprehensive approach instead of individual training activities. Besides, specific regions might face specific demands, which would require regionally tailored efforts.

However, the proposed efforts do not address the capacities needed for the implementation of certain norms and CBMs proposed by the GGE and the three regional organisations. In particular, there is a need for developing capacities in the field of reducing the risk of misperception and escalating tensions, through activities targeting high-level decision-makers as well as diplomats on a broader set of cybersecurity aspects, and especially on the application of international law to cyberspace, operational mechanisms, and co-operation with stakeholders.

Conclusion

The fast-changing online environment, driven by the marked demand for ever more powerful rather than more secure products, results in an increasing number of intrinsic vulnerabilities in software and hardware. The flourishing cybercrime markets have exploited these vulnerabilities to create an abundance of cyber-weapons that are readily available and easy to use – yet potentially causing detrimental consequences for their targets and society in general. The increasing interest of states in cyber-armament as a potential means of defending society's critical resources and infrastructure, is accompanied with their growing capacity to produce highly sophisticated offensive tools based on discovered or purchased exploits. The lack of widely agreed norms of state behaviour in cyberspace, as well as the lack of common terminology used to discuss cyber issues, is increasing the risks of possible misperception which could escalate cyber-incidents into conflicts.

In response to frequent cyber-attacks, including those less-visible involving intrusion into computer systems of state agencies, the corporate sector, and CI, states are turning to bilateral relations and agreements. The existing multilateral frameworks – and particularly the UN GGE, the OSCE, ASEAN Regional Forum, and the OAS – have the potential to galvanise the willingness of governments to explore venues of co-operation on cyber issues and reduce the risk of cyber-conflicts.

There are several important considerations arising from the analysis of existing frameworks that might be fed into the further development of the norms and measures by the GGE and regional forums. In addition, the side-event of the second meeting of the UN GGE titled 'Towards a Secure Cyberspace via Regional Co-operation', organised in Geneva on 30 November 2016 by the Federal Department of Foreign Affairs of Switzerland, in co-operation with the Geneva Internet Platform, brought about number of important views.[72]

Inclusiveness and outreach

The outreach of the GGE's work may be enhanced, allowing other countries to better understand its work and contribute to the operationalisation and implementation of the proposed measures. At the same time, a mechanism may be discussed to provide an opportunity for states outside of the GGE, as well as other stakeholders, to contribute to the process. Particularly important is the interplay between the GGE and the regional organisations.

The efficient operationalisation of the norms and CBMs may also require greater involvement of other stakeholders in the work of both the GGE and the regional fora.[73] Some CBMs and norms invite for a certain (appropriate) level of involvement from the private sector and civil society, especially in relation to protection of CI and response to incidents. A more comprehensive approach by all fora may be needed towards substantial involvement of the Internet industry, civil society, academic institutions, and the technical community in all other areas - such as to combat cybercrime, reduce the risk of escalations, build capacity, and develop research.

Policy coherence

Analysis of existing measures confirms the relevance of each of the frameworks: the norms developed by the GGE provide strategic guidance, shape the foundations of the international cybersecurity environment and serve as a basis for confidence and trust, while the CBMs developed at regional levels enable the operationalisation of those through practical co-operation and communication measures, taking into consideration the social, cultural, and political specificities of the regions. There is also the potential for regional CBMs to strengthen global processes – including the GGE – by raising regional concerns and highlighting possible sensitivities and concerns related to regional adherence to international norms.

To maximise the effects of various efforts, there is a need for policy coherence on two levels: vertical and horizontal. *Vertically*, the measures shaped on global, regional, multilateral, and bilateral levels should co-exist in a coherent way. To that end, enhanced communication and co-operation across the regions and among the regional organisations,[74] as well as with the UN GGE, is crucial; at the same time, the regional organisations should get mandate from their member states to implement the GGE recommendations. *Horizontally*, the measures related to cybersecurity should be coherent with policies and endeavours in other fields which interact with security, as per the UN policy trinity: peace and security, economic development, and human rights. Both the UN GGE and regional forums could benefit from a multidisciplinary consideration of cybersecurity issues.

Comprehensive capacity building

Capacity building can be seen as a third pillar of international cybersecurity policy, along with rules and confidence building activities, and is clearly recognised by the GGE and the OSCE, ARF, and the OAS. They also recognise that the implementation of norms and CBMs is not possible without strong capacity by states and other stakeholders.

Specific proposed measures outline a multidisciplinary palette of knowledge – related to technology, legislation, and diplomacy – to address preparedness, respond to incidents, avoid miscommunications, and implement international law. In addition, the norms and CBMs themselves require a holistic understanding of the cyber en-

[72] The report from the event is available at: https://www.diplomacy.edu/blog/towards-secure-cyberspace-regional-cooperation

[73] The session 'NetGov, Please Meet Cybernorms. Opening the debate' organised during the 11th Internet Governance Forum of the United Nations, held 5-9 December 2016, also outlined an important role that other stakeholders, in particular the technical community, may play in operationalisation of the norms and CBMs. The report from the session is available at: http://digitalwatch.giplatform.org/sessions/ws132-netgov-please-meet-cybernorms-opening-debate

[74] One example is the OSCE-Asia Conference. More information is available at: http://www.osce.org/partners-for-cooperation/asian/236731

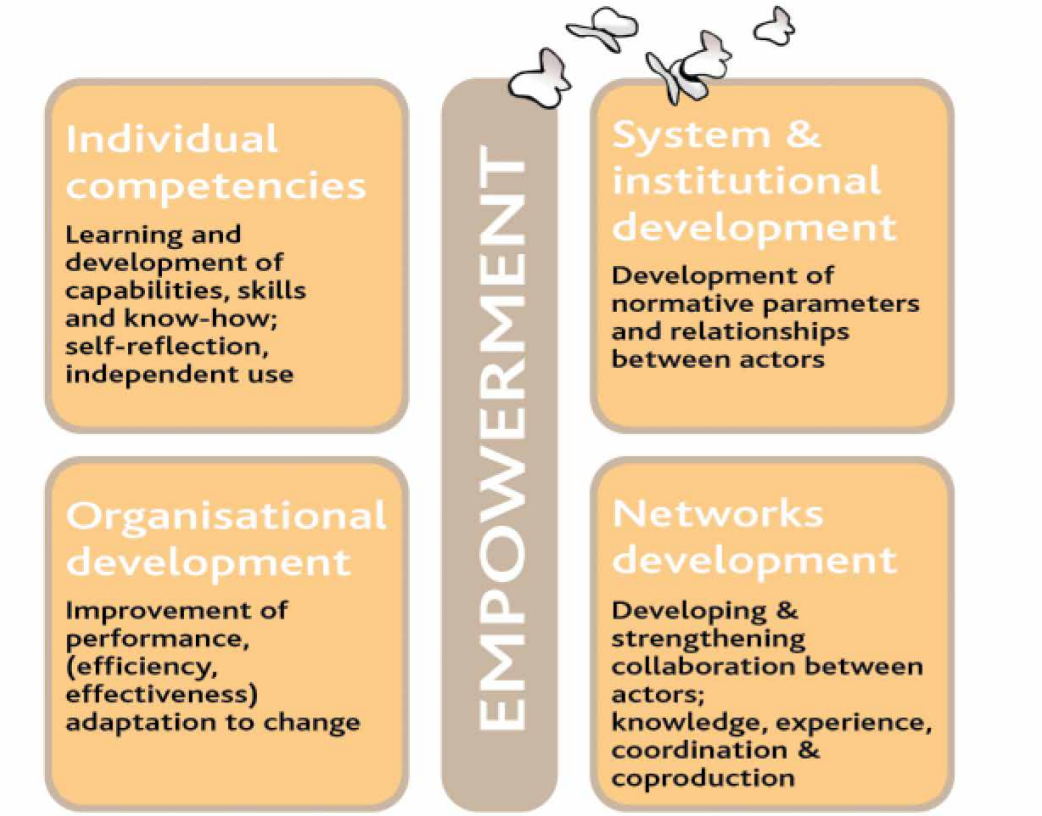


Figure 3. Capacity development 'butterfly'

Swiss Agency for Development and Cooperation (2006) Capacity Development in SDC. Available at https://www.eda.admin.ch/content/dam/deza/en/documents/die-deza/strategie/202114-capacity-development-sdc_EN.pdf

vironment by involved stakeholders, including topics outside the narrow scope of security – in particular, human rights, freedoms, economic growth, and development. Not least, the number of measures clearly calls for sustainability of capacity-building endeavours, including through budgetary planning, devotion of and investments by states and regional organisations, and the involvement of the private sector, civil society, and academia in conceptualising and implementing the programmes.

Development of hard and soft capacities requires carefully designed training, coaching, and organisational-building activities. In addition, to be effective and comprehensive, capacities need to be developed on various levels. The capacity development 'butterfly' (Figure 5), based on the methodology used by the Swiss Agency for Development and Cooperation, offers important insights into the complexity of the efforts.

As the debates on cyber policies have shifted towards a more mature phase, a stronger focus on organisational development is required, which includes developing the organisational capacities of governments, civil society, business associations, and academia among others. In particular:

- Capacity building should reflect local cyber dynamics, taking into consideration local political, social, cultural, and other specific conditions in developing and implementing capacity-development programmes and activities.
- Existing cybersecurity training activities should be enriched by – for example – adding sessions on legal and economic aspects of cybersecurity to pure technical training, and vice-versa.
- The urgency for cybersecurity capacity building could be addressed by providing just-in-time learning as a part of policy processes. Some elements of this approach are used by DiploFoundation and the GIP, in just-in-time training programmes for diplomats, as well as dedicated programmes for newcomers within ICANN, as part of its Fellowship Programme,[75] and the Internet Society, as part of the Internet Governance Forum Ambassadors Programme.[76]
- Longer capacity-building impact should be achieved on a systematic level, by including cybersecurity aspects as well as digital literacy in the curriculum of academic and professional training centres.

The GGE and the regional forums should continue to outline key capacity-building requirements and needs, and propose particular co-operation measures. More importantly, they should also move out of normative ground into the practical implementation of comprehensive capacity-building programmes, in partnership with academic institutions, civil society, capacity-building and training organisations, the private sector, and the technical community.

[75] ICANN (no date) ICANN Meeting Fellowships. Available at https://www.icann.org/fellowshipprogram

[76] Internet Society (no date) IGF Ambassadors Programme. Available at https://www.internetsociety.org/what-we-do/education-and-leadership-programmes/next-generation-leaders/igf-ambassadors-programme

Malta
DiploFoundation
Anutruf, Ground Floor
Hriereb Street
Msida, MSD 1675, Malta

Switzerland
DiploFoundation
7bis, Avenue de la Paix
CH-1211 Geneva, Switzerland

Serbia
DiploCentar
Braničevska 12a/12
11000 Belgrade, Serbia

DiploFoundation's cybersecurity initiatives
www.diplomacy.edu/cybersecurity

Cybersecurity on the GIP Digital Watch observatory
http://digitalwatch.giplatform.org/issues/cybersecurity