DiploFoundation

Geneva Dialogue for Responsible Behaviour in Cyberspace

in the context of international peace and security

Research introductory document

May 2018

Authors:
Irina Rizmal and Vladimir Radunovic, DiploFoundation

Contents

DiPLO
www.diplomacy.edu

Introduction

Cybersecurity is an ever-present global issue which national governments cannot deal with on their own. Despite a global consensus on the need for engaging a plethora of additional actors in cybersecurity provision, there is no common approach nor framework for such an endeavour. Instead, approaches related to non-state actors' inclusion vary in format and scope across countries and regions. Initiatives for various forms of cooperation on cybersecurity arise equally among government, the private sector and technical community, academia, as well as civil society and, ultimately, end-users. In order to develop a functional framework for these actors to assume, or be attributed with, specific roles in the cyber ecosystem, a general taxonomy needs to be developed, based on an overview of various existing approaches, in order to identify best practice.

The Geneva Dialogue for Responsible Behaviour in Cyberspace aims to do precisely this. By mapping the roles and obligations pertaining to responsible behaviour in cyberspace of different actor clusters, the project provides a comprehensive contribution to this ongoing debate. The clusters of roles and responsibilities presented within this research are drawn from an extensive list of policy documents and frameworks, proposals, initiatives, programmes, researches and analyses developed, agreed and promoted by international and intergovernmental organisations, private enterprise and corporations, the technical and academic community, think-tanks and civil society organisations. Attributed, assumed and proposed roles and responsibilities are all included. A differentiation between those stemming from the actor cluster at hand, and the roles and responsibilities expected to be assumed by that cluster from the rest of the stakeholder community is made. As such, the research developed within this project serves as a baseline for an inclusive dialogue to take place among the stakeholder community on the specific roles and obligations to be embraced by each actor cluster, with the aim of developing a comprehensive operational framework for responsible behaviour in cyberspace.

The actors and resources consulted throughout the research process are found as most relevant given the research topic at the time of writing this paper. However, given the pace of change in the field of cybersecurity, it is important to keep in mind that the list presented is neither exclusive nor final. Instead, the format of the research allows for it to be updated and expanded as new actors and/or resources arise in the field. The research thus serves as a starting point for developing a wider dialogue on the responsibilities and roles assumed by, or attributed to, various actors in the field of cybersecurity.

The document in front of you poses as an introductory paper to the wider research conducted by DiploFoundation as part of this project. It details the research process, the methodology used, as well as the preliminary clusters of actors and roles and obligations arrived at. The structure of the paper mirrors this aim. The following chapters detail the clusters of actors developed from within the stakeholder community, followed by a brief explanation of the methodology used and the research sample consulted. Finally, a general overview of the mapped roles and responsibilities promoted within the sample is provided. The paper concludes with a section briefly explaining the next steps of this project.

Brief note on the methodology and research sample

Examining the roles and responsibilities different actors propose, assume or are attributed with within cybersecurity frameworks require an approach that allows immersion in the sampled data in much depth and detail. For this reason, Qualitative Content Analysis (QCA) is employed, allowing development of broad themes and specific clusters of roles and responsibilities based on the inspected documents, initiatives and programmes, summarising the content analysed.

Approaching each resource analysed as an individual unit of analysis, different *codes* are developed as descriptive categories or the specific roles and responsibilities defined. This allows clustering similar identified codes into broader categories, arriving eventually at a comprehensive taxonomy of roles and obligations of different actor clusters identified in the sample pertaining to responsible behaviour in cyberspace.

For the purpose of this research, responsible behaviour in cyberspace, in the context of international peace and security, is understood as adopting a wider approach than mere focus on imminent threats of conflict and/or attacks. Instead, it encompasses an acknowledgement of permanent and overarching risks, impacting relations and stability between and across societies and economies. These two cannot be approached separately, especially in times of increased dominance of hybrid threats.

In terms of the sample itself, 70+ resources have been analysed for the purpose of this research, both adopted and proposed by the range of actors identified in the previous section. Only the roles and responsibilities that are clearly defined and attributed to a specific actor are taken into account, coded and included in the developed clusters. Overall, 280 defined roles and responsibilities have been mapped. For clarity and transparency reasons, a *Codebook* that explain the logic of the clustering process of mapped roles and responsibilities are provided in Appendix 2.

Classification of Actors

For the purpose of this research, three broad clusters of actors are identified within the stakeholder community. These include states, private sector actors and a general group of actors defined as communities and individuals. More specifically, this means that the stakeholders are seen as consisting of:

- States, whereby primary focus for the purpose of this research is placed on regional, intergovernmental and international organisations and regimes, analysing the agreements and initiatives adhered to, adopted or proposed by a number of different states;
- Private sector actors, consisting of corporations and enterprise, whereby the initiatives adopted or promoted by this actor cluster at both the regional and international level are consulted, including also attempts at self-regulation with reference to responsible behaviour in cyberspace; and
- Communities and individuals, encompassing the expert, technical community and associations, think-tanks, foundations and civil society organisations (as non-profits), as well as the academic sector (including universities and academic research centres).

Initiatives launched within the framework of public-private partnerships are also addressed, posing as an intersection of efforts aimed at ensuring responsible behaviour and maintaining peace and security in cyberspace.

A specific note must be made regarding the positioning of Computer Emergency Response Teams (CERTs). Although rarely addressed in the research sample other than in reference to the role of states to establish such frameworks, it is important to note that CERTs can fall both into all three actor clusters. Even national CERTs can be seen as independent bodies primarily with technical roles, and therefore posing rather as a member of the broader stakeholder pool – as part of the technical community; while in other instances they are seen as a potential political and diplomatic tool, placed within public institutions and bodies, without significant independence. In addition, CERTs can also provide commercial services, or act as sector-specific CERTs, for example, providing services to specific sectors, such as media and civil society organisations. This question is, for the time being, placed within questions for broader consideration in this project phase.

Such actor clusters are developed based on comprehensive inspection of a variety of documents dealing with the focus topic, and the differentiation these make when discussing key stakeholder groups in cybersecurity. Documents developed by all listed stakeholders have been consulted for this purpose. A comprehensive list of the actors and the specific documents in which such classifications are developed is presented in Appendix 1.

Classification of Roles and Responsibilities

For the purpose of identifying current roles and responsibilities – both proposed and already assumed – of identified actors in the stakeholder community, existing normative resources in the form of executive decisions, declarations and directives, as well as voluntary measures, codes of conduct and conventions proposed and/or adopted by the previously listed actors have been inspected. These document enable both examining the roles different actors are attributed with, in the case of normative documents for example, as well as the responsibilities and roles they individually assume, in the case of specific-sector initiatives. The communities and users cluster, as defined in this paper, is also seen as quite active in both assuming a growing role in peace and security in cyberspace debates and actions, but also in suggesting potential roles and responsibilities of other actor clusters, due to its expertise and research capacity.

As outlined in the previous section, the specific clusters of existing roles and responsibilities – both assumed and proposed – are developed through the process of coding the documents inspected as the research sample. A preliminary list of mapped clusters includes the following roles and responsibilities:

- Developing and adopting a national/organisational cybersecurity framework, encompassing activities such as setting the normative frameworks, further policy and strategy development, establishment of Computer Emergency Response Teams (CERTs) and National Points of Contact, as well as establishment of public-private partnerships.
- Awareness raising among the private sector and the general public through adopting comprehensive approaches and campaign development, training and education, capacity building and engagement in public-private partnerships in order to reach wider audiences with information on threats and risks in cyberspace as well as methods to ensure their own security.

- Capacity building of states, the private sector, small and medium enterprises, the workforce, and the general public, through training and education, awareness raising, and international cooperation in order to develop baseline capabilities for implementing standards and norms for cybersecurity and responsible behaviour in cyberspace.
- Cooperation, including national-level public-private partnerships, bilateral, sub-regional, regional and international, through information sharing and incident response, self-regulation, standard development, transparency and accountable behaviour, fostering more efficient and comprehensive cybersecurity frameworks.
- Norm development, including codes of practice, standards, confidence-building measures (CBMs), through regulation and self-regulation, international cooperation, and public-private partnerships, establishing baseline patterns for responsible behaviour in cyberspace.
- Development of, and engagement in, public-private partnerships aimed at fostering capacity building, development of cybersecurity frameworks, awareness raising, cooperation and information sharing, collective action, provision of cybersecurity, as well as ensuring responsible behaviour of the actors involved.
- Ensuring security of cyberspace, including ensuring own security, national security as well as broader, international security by acting on intelligence obtained, correcting software vulnerabilities and following 'security by design' principles, maintaining cyber hygiene, providing cyber defence, engaging in public-private cooperation, cooperation and responsible behaviour, information sharing, awareness raising and capacity building, as well as through establishment of cybersecurity frameworks in general.
- Policy development in terms of setting national cybersecurity frameworks, developing specific and enforceable regulations and standards for all national stakeholders involved.
- Responsible behaviour, which can be further divided into two strands. First, there are negative responsibilities that refer to actors refraining from doing something, such as ensuring *not to* engage in malicious activities. These form the very basis of responsible behaviour. Second, there are positive responsibilities that refer to notions of transparency and accountability, taking responsibility for attributable actions, developing comprehensive cybersecurity frameworks, depoliticising specific aspects of cybersecurity frameworks and, fundamentally, taking into account human rights concerns.

All of these are presented through further two strands in the final baseline documents. First, those that are proposed, assumed by or attributed to an actor cluster by the actors falling into that specific category are presented. In addition, the roles and responsibilities other actors believe the actor cluster at hand should assume are also outlined. This sets out the basis for a broader multi-stakeholder discussion in roles and responsibilities for a safe cyberspace dialogue, which is the ultimate aim of the project.

The list of documents, initiatives and programmes forming the core of the research sample is presented in Appendix 3.

Next steps

This baseline research develops specific clusters of actors and roles and responsibilities they have in the cybersecurity ecosystem, with specific focus on contributing to and maintaining international peace and security. The clusters are developed based on the commonality of the types of actors and their roles and responsibilities, ranked by the frequency with which they occur in the frameworks inspected.

This baseline research sets the ground for an inclusive multi-stakeholder consultation process consisting of representatives of states, private sector corporations and enterprises, the wider technical community, academia, think-tanks and civil society organisations. With each identified actor cluster presented with a baseline document listing existing assumed and proposed roles and responsibilities, stemming both from its own stakeholder cluster, as well as providing a view of its obligations according to other actor clusters, a fruitful debate can take place on a joint cross-sector approach to ensure stability, peace and security in cyberspace. Based on the findings, fact-based conclusions on existing roles and responsibilities of actors can be drawn, at the same time identifying potential overlaps and gaps affecting operational capacity of the cybersecurity ecosystem. From there, further initiatives aimed at developing standards and norms of responsible behaviour in cyberspace can be made from an informed, fact-based standpoint, which is the ultimate aim of this project.

Appendix 1: Existing classifications/deliberations on Actors

Regional, intergovernmental and international organisations

African Union: '*..each State Party undertakes to promote the culture of cyber security among all stakeholders, namely governments, enterprises and the civil society..*'[1]

Asia Pacific Economic Cooperation: '*..outreach to economies, industry and consumers regarding cybersecurity and cyberethics should be conducted..*'[2]

Asia Pacific Economic Cooperation: '*..stakeholder groups included ISPs, and peak industry groups, government agencies and ministries, and Computer Emergency Response Teams (CERTs). Effective strategies for engaging consumers should also be considered..*'[3]

Asia Pacific Economic Cooperation: '*..engage governments, the private sector, other..*'[4]

Association of Southeast Asian Nations: '*..policy officials, diplomats, prosecutors as well as technical operators and analysts. It expects involvement of industry, NGOs and academia..*'[5]

NATO Cooperative Cyber Defence Centre of Excellence: '*..while recognising that decision makers, in particular military staff and diplomats, are the primary addressees of the CBMs, one cannot ignore the*

[1] African Union Convention on Cyber Security and Personal Data Protection. 2014. African Union.
[2] APEC Cybersecurity Strategy. 2002. Asia Pacific Economic Cooperation.
[3] APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice. 2011. Asia Pacific Economic Cooperation.
[4] APEC Telecom and Information Working Group. Strategic Action Plan 2016-2020. 2015. Asia Pacific Economic Cooperation.
[5] ASEAN Cyber Capacity Programme. 2016. Association of Southeast Asian Nations.

fact that in order to take informed decisions, they need to rely on and interact with technical experts, law enforcement agencies and the private sector..'[6]

Commonwealth: '*..appropriate consultative processes involving industry, academia, governments and other relevant stakeholders..'*[7]

Commonwealth: '*..[member countries will] working with relevant international organisations, the private sector, academic institutions, Commonwealth initiatives and their shareholders..'*[8]

Commonwealth Telecommunications Organisation: '*..including policy makers, officials from across most government departments, specific agencies, private sector representatives from many industries, civil society, academics, international bodies and possibly other countries..'*[9]

Commonwealth Telecommunications Organisation: '*..governments, industry, civil society and users have a shared responsibility..'*[10]

European Union: '*..bring together the European External Action Service (EEAS), Member States' cyber authorities, EU agencies, Commission services, academia and civil society..'*[11]

European Union: '*..alongside industry, state administration, national bodies for standardisation, the users' community and academia, the Governance Framework also lists transnational European Standardisation Organisations (ESOs) as recognised by the European Commission..'*[12]

G7: '*..cooperation and collaboration, both nationally and internationally, of the various actors responsible for cyber security, cyber defence and fighting cybercrime, including businesses, research and societies as a whole..'*[13]

International Telecommunications Union: '*..invites Member States, Sector Members, Associates and Academia..'*[14]

International Telecommunications Union: '*..encouraging academia to provide for the education.. […] ..allowing governments, businesses, civil society and individual users to work together..'*[15]

---

[6] Confidence-Building Measures in Cyberspace: Current Debates and Trends. 2016. In Osula, A. M. and Roigas, H. (eds.) International Cyber Norms. North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence.

[7] Commonwealth Cyber Declaration. 2018. The Commonwealth.

[8] Ibid.

[9] Commonwealth approach for developing national cybersecurity strategies. 2015. Commonwealth Telecommunications Organisation.

[10] Commonwealth Cybergovernance Model. Commonwealth ICT Ministers forum 2014. Commonwealth Telecommunications Organisation. 2014.

[11] Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 13.9.2017. JOIN(2017) 450 final.

[12] Governance Framework for European Standardisation: Aligning policy, industry and research. December 2015. European Union Agency for Network and Information Security.

[13] The principles and actions on cyber. 2016. Group of 7 (G7).

[14] Resolution 45. Mechanisms for enhancing cooperation on cybersecurity including countering and combating spam. 2014. International Telecommunications Union.
Resolution 50. Cybersecurity. 2016. International Telecommunications Union.

[15] The role and responsibilities of an effective regulator. 2009. International Telecommunications Union.

Organisation of American States: '*..promoting public sector cooperation with the private sector and academia..*'[16]

Organisation for Economic Cooperation and Development: '*.."stakeholders" are considered as "the governments, public and private organisations, and the individuals, who rely on the digital environment..*'[17]

Organisation for Security and Cooperation in Europe: '*..Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society..*'[18]

Shanghai Cooperation Organisation

: '*..all States must cooperate fully with other interested parties in encouraging a deeper understanding by all elements in society, including the private sector and civil-society institutions..*'[19]

United Nations Group of Governmental Experts: '*..States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations..*'[20]

Private sector corporations and enterprise

Microsoft: '*..norms are an imperative for all users, governments, the private sector, non-governmental organizations (NGOs), and individuals, in an Internet-dependent world.. […] ..allow for strong input by the private sector, academia, and civil society..*'[21]

Microsoft: '*..support civil society, governments and international organizations in their efforts to advance security in cyberspace.. […] .. establish formal and informal partnerships with industry, civil society, and security researchers..*'[22]

Broader civil society

[16] Declaration strengthening cyber-security in the Americas. 2012. Organisation of American States.
[17] Digital security risk management for Economic and Social Prosperity. OECD Recommendations and Companion document. 2015. Organisation for Economic Cooperation and Development.
[18] Decision No.1202. OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. 2016. Organisation for Security and Cooperation in Europe. PC.DEC/1202.
[19] International Code of Conduct for Information Security. 2015. Shanghai Cooperation Organisation.
[20] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2015. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174.
[21] International Cybersecurity Norms. 2016. Microsoft.
[22] A Tech Accord to protect people in cyberspace. 2018. Microsoft.

Atlantic Council: '*..States are not the only […] actors in cyberspace.. […] ..role of companies, nongovernmental organizations, civil society, and others..*'[23]

Global Commission on Internet Governance: '*..four classes of actors: states, formal intergovernmental organizations (IGOs), firms and civil society actors..*'[24]

Global Commission on the Stability of Cyberspace: '*..governments, private sector and civil society as the main stakeholders.. […] ..today, the technical-academic community is seen as a fourth key stakeholder..*'[25]

Global Forum on Cyber Expertise: '*..including governments, international organisations, private companies, civil society, technical community and academia..*'[26]

World Federation of Scientists: '*..governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs..*'[27]

World Economic Forum: '*..public-private partnerships [of the Government] with civil society and academia can also help..*'[28]

[23] Confidence-building measures in cyberspace. A multistakeholder approach for stability and security. 2014. Atlantic Council.

[24] Multi-stakeholderism: Anatomy of an Inchoate Global Institution. 2016. Global Commission on Internet Governance.

[25] Towards a holistic approach for internet related public policy making. 2017. Global Commission on the Stability of Cyberspace.

[26] Delhi communique on a GFCE global agenda for cyber capacity building. 2017. Global Forum on Cyber Expertise.

[27] Erice Declaration on Principles for Cyber Stability and Cyber Peace. 2009. World Federation of Scientist.

[28] Global Agenda Council on Cybersecurity. 2016. White Paper. World Economic Forum.

Appendix 2: Codebook of clustered roles and responsibilities

Developed cluster	Description	Mapped categories/examples
Adopt cybersecurity framework	Developing and adopting a national/organisational cybersecurity framework, encompassing activities such as setting the normative frameworks, further policy and strategy development, establishment of Computer Emergency Response Teams (CERTs) and National Points of Contact, as well as establishment of public-private partnerships	"*..governments, for their part, should develop national strategies and adopt public policy initiatives and measures to foster digital security risk management among all stakeholders*.." OECD "*..develop […] a national cybersecurity policy which recognises Critical Information Infrastructure (CII) […] identifies risks […] and outlines how the objectives of such policy are to be achieved […] adopt strategies they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity-building, public-private partnership and international cooperation [...] define organisational structures, set objectives and timeframes..*" African Union
Awareness raising	Awareness raising among the private sector and the general public through adopting comprehensive approaches and campaign development, training and education, capacity building and engagement in public-private partnerships in order to reach wider audiences with information on threats and risks in cyberspace as well as methods to ensure their own security	"*..bolster outreach campaigns by specifically targeting those populations without dedicated IT staffs (home users, older adults, students, small businesses) with awareness videos, commercials, and free help…*" Information Technology Industry Council "*..formulate a 'business case' for information security that assists corporations with their network security efforts and explains the economic reasons behind developing sound network security practices..*" APEC

Capacity building	Capacity building of states, the private sector, small and medium enterprises, the workforce, and the general public, through training and education, awareness raising, and international cooperation in order to develop baseline capabilities for implementing standards and norms for cybersecurity and responsible behaviour in cyberspace	*"..help educate businesses and consumers on how to protect their connections […] help the industry maximize the advantages of IoT while educating about how to keep companies and consumers more secure.."* IoT Cybersecurity Alliance *"..calls on governments and public and private organisations to work together to empower individuals and small and medium enterprises to collaboratively manage digital security risk.."* OECD
Cooperation	Cooperation, including national-level public-private partnerships, bilateral, sub-regional, regional and international, through information sharing and incident response, self-regulation, standard development, transparency and accountable behaviour, fostering more efficient and comprehensive cybersecurity frameworks	*"..endeavour to strengthen our cooperation to promote security and stability in cyberspace, including through the promotion of cooperation among national computer security incident response teams, capacity building, and awareness raising.."* G7 *"..those of us in the tech sector need to act collectively to better protect the internet and customers everywhere from nation-state attacks.."* Microsoft

Norm development	Norm development, including codes of practice, standards, confidence-building measures (CBMs), through regulation and self-regulation, international cooperation, and public-private partnerships, establishing baseline patterns for responsible behaviour in cyberspace	"*..provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term […] in the longer term, participating States will endeavour to produce a consensus glossary..*" OSCE "*..commit to promote frameworks for cyberspace, including the applicability of international law, agreed voluntary norms of responsible state behaviour, and the development and implementation of confidence building measures..*" The Commonwealth
Establishment of public-private partnerships	Development of, and engagement in, public-private partnerships aimed at fostering capacity building, development of cybersecurity frameworks, awareness raising, cooperation and information sharing, collective action, provision of cybersecurity, as well as ensuring responsible behaviour of the actors involved	"*..combine domain knowhow and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.e. contractual Public Private Partnerships..*" Siemens "*..cooperate fully with other interested parties in encouraging a deeper understanding by all elements in society, including the private sector and civil-society institutions..*" Shanghai Cooperation Organisation

Ensuring security	Ensuring security of cyberspace, including ensuring own security, national security as well as broader, international security by acting on intelligence obtained, correcting software vulnerabilities and following 'security by design' principles, maintaining cyber hygiene, providing cyber defence, engaging in public-private cooperation, cooperation and responsible behaviour, information sharing, awareness raising and capacity building, as well as through establishment of cybersecurity frameworks in general	"*..obligation to help protect the Internet and systems that support their economies, enrich the lives of their citizens, and support government and military operations..*" East-West Institute "*..defence is a role more naturally suited for government, given the exercise of sovereign responsibilities, laws and regulations related to intentionally doing harm to another individual or entity, and the economic profile of developing defence capabilities..*" World Economic Forum "*..protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical..*" Microsoft "*..enhancing the security and resilience of critical information and communications technology (ICT) infrastructure against cyber threats, with a particular focus on critical governmental institutions as well as those sectors critical to national security..*" Organisation of American States
Policy development	Policy development in terms of setting national cybersecurity frameworks, developing specific and enforceable regulations and standards for all national stakeholders involved	"*..the Internet technical community notes, with the civil society, that governments can play a lead role in the implementation of best practices, including policies, technologies and even legislative requirements to secure their own information systems and networks..*" OECD "*..academics serve a very useful role by helping develop critical intellectual capital that is needed in the cyber policy community..*" Hewlett Foundation

Responsible behaviour	Responsible behaviour, which can be further divided into two strands. First, there are negative responsibilities that refer to actors refraining from doing something, such as ensuring *not to* engage in malicious activities. These form the very basis of responsible behaviour. Second, there are positive responsibilities that refer to notions of transparency and accountability, taking responsibility for attributable actions, developing comprehensive cybersecurity frameworks, depoliticising specific aspects of cybersecurity frameworks and, fundamentally, taking into account human rights concerns	"*..private companies themselves have increasingly been called to task by United Nations human rights bodies (as well as non-United Nations groups) for the role they play in exacerbating human rights and privacy concerns, particularly during moments of political instability and crisis..*" UNIDIR "*..critical that countries begin to refashion their domestic statutes to take into consideration the legitimate privacy interests of both individuals outside of their country and the comity interests of the countries in which those individuals are citizens..*" Google "*..without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace..*" Global Commission on Internet Governance

Appendix 3: Research sample

Regional, intergovernmental and international organisations

African Union Convention on Cyber Security and Personal Data Protection. 2014. African Union.

APEC Cybersecurity Strategy. 2002. Asia-Pacific Economic Cooperation.

APEC Telecom and Information Working Group. Strategic Action Plan 2016-2020. 2015. Asia-Pacific Economic Cooperation.

APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice. 2011. Asia-Pacific Economic Cooperation.

ASEAN Regional Forum Work Plan on Security of and use of Information and Communication Technologies (ICTs). 2015. Association of Southeast Asian Nations.

ASEAN Cyber Capacity Programme. est.2016. Association of Southeast Asian Nations.

ASEAN ICT Master Plan 2020. 2015. Association of Southeast Asian Nations.

ASEAN Leaders' statement on cybersecurity cooperation. 2018. Association of Southeast Asian Nations.

The 6th BRICS Summit: Fortaleza Declaration. 2014. BRICS economies.

Dubai Action Plan 2015-2017. 2015. Commonwealth of Independent States.

Commonwealth Cyber Declaration. 2018. The Commonwealth.

Commonwealth Cybergovernance Model. Commonwealth ICT Ministers forum 2014. 2014. Commonwealth Telecommunications Organisation.

Commonwealth approach for developing national cybersecurity strategies. 2015. Commonwealth Telecommunications Organisation.

Strategic Plan of the Commonwealth Telecommunications Organisation (CTO) for the period 2016-2020. 2016. Commonwealth Telecommunications Organisation.

Commission recommendation of 13.9.2017. on Coordinated Response to Large Scale Cybersecurity Incidents and Crises. European Commission. C(2017) 6100 final.

Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). European Commission. COM(2017) 477 final. 2017/0225 (COD).

Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 13.9.2017. European Commission. JOIN(2017) 450 final.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (NIS Directive) L194/1

Governance framework for European standardisation: Aligning Policy, Industry and Research. December 2015. European Union Agency for Network and Information Security.

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013. European Union External Action Service. JOIN(2013) 1 final.

Chair's Statement. 2017. Global Conference on Cyberspace.

Chair's Statement. 2015. Global Conference on Cyberspace.

Chair's Statement. 2011. Global Conference on Cyberspace.

G7 Declaration on responsible states behaviour in cyberspace. 2017. Group of 7 (G7).

The principles and actions on cyber. 2016. Group of 7 (G7).

G7 fundamental elements for effective assessment of cybersecurity in the financial sector. 2016. Group of 7 (G7).

Progress update on Cyber Lexicon. Report to 19-20 March 2018 G20 Finance Ministers and Central Bank Governors Meeting Buenos Aires, Argentina. Financial Stability Board. 2018. Group of 20 (G20).

Antalya Summit declaration. G20 Leaders' Communique. 2015. Group of 20 (G20).

The role and responsibilities of an effective regulator. 2009. International Telecommunications Union.

Resolution 45. Mechanisms for enhancing cooperation on cybersecurity including countering and combating spam. 2014. International Telecommunications Union.

Resolution 130. Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. 2014. International Telecommunications Union.

Resolution 50. Cybersecurity. 2016. International Telecommunications Union.

NATO Industry Cyber Partnership (NICP). North Atlantic Treaty Organisation.

Adoption of a comprehensive Inter-American Strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity. 2004. Organisation of American States.

Recommendations of the CICTE cybersecurity practitioners' workshop on the OAS integral cybersecurity strategy: Framework for establishing the Inter-American CSIRT watch and warning network. 2004. Organisation of American States.

Declaration strengthening cyber-security in the Americas. 2012. Organisation of American States.

Establishment of a working group on cooperation and confidence-building measures in cyberspace. 2017. Organisation of American States (Inter-American Committee Against Terrorism – CICTE).

Cybersecurity policy making at a turning point. 2012. Organisation for Economic Cooperation and Development.

Digital security risk management for Economic and Social Prosperity. OECD Recommendations and Companion document. 2015. Organisation for Economic Cooperation and Development.

Decision No.1106. initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. 2013. Organisation for Security and Cooperation in Europe. PC.DEC/1106.

Decision No.1202. OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. 2016. Organisation for Security and Cooperation in Europe. PC.DEC/1202.

Astana Declaration. 2017. Shanghai Cooperation Organisation.

International Code of Conduct for Information Security. 2015. Shanghai Cooperation Organisation.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2010. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2013. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98*.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2015. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174.

Report of the International Security Cyber Issues Workshop Series. 2016. United Nations Institute for Disarmament Research.

UN cyberspace and international peace and security. 2017. United Nations Institute for Disarmament Research.

Voluntary, non-binding norms for responsible state behaviour in the use of information and communications technology. A commentary. 2017. United Nations Office for Disarmament Affairs.

World Summit on the Information Society. 2005. Tunis Agenda for Information Society.

Private sector corporations and enterprise

IoT Cybersecurity Alliance. 2017. AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic.

Notifications for targeted attacks. 2015. Facebook.

Security warnings for suspected state-sponsored attacks. 2012. Google.

Digital Security and Due Process: Modernising cross-border government access standards for the cloud era. 2017. Google.

Yahoo to notify its users about 'state-sponsored' hacking attacks. 2015. The Guardian.

Additional steps to help keep your personal information secure. 2015. Microsoft.

From Articulation to Implementation: Enabling progress on cybersecurity norms. 2016. Microsoft.

International Cybersecurity Norms. 2016. Microsoft.

The need for a Digital Geneva Convention. 2017. Microsoft.

Cybersecurity Tech Accord. 2018. Microsoft.

A Tech Accord to protect people in cyberspace. 2018. Microsoft.

SAFECode Fundamental Practices for Secure Software Development. 2018. SAFECode.

Charter of Trust. For a secure digital world. 2018. Siemens.

Communities and users

Confidence-building measures in cyberspace. A multistakeholder approach for stability and security. 2014. Atlantic Council.

Healey, J. Breaking the Cyber-Sharing Logjam. 2015. Atlantic Council.

Getting beyond norms. New approaches to international cyber security challenges. 2017. Centre for International Governance Innovation.

Rights and responsibilities in cyberspace. 2010. Balancing the need for security and liberty. East-West Institute.

Exploring Multi-Stakeholder Internet Governance. 2015. East-West Institute.

The proposed Digital Geneva Convention: Towards an inclusive public-private agreement on cyberspace? 2017. Geneva Centre for Security Policy.

Hybrid politics in Europe. 2018. Geneva Centre for Security Policy.

Multi-stakeholderism: Anatomy of an Inchoate Global Institution. 2016. Global Commission on Internet Governance.

Briefings from the Research Advisory Group. 2017. Global Commission on the stability of cyberspace.

Call to Protect the Public Core of the Internet. 2017. Global Commission on the Stability of Cyberspace.

Delhi communique on a GFCE global agenda for cyber capacity building. 2017. Global Forum on Cyber Expertise.

Good neighbours make good security: Coordinating EU critical infrastructure protection against cyber threats. 2017. GLOBSEC.

Kavanagh, K. and Stauffacher, D. 2014. A Role for Civil Society? ICT4Peace Foundation.

Global Internet Report. 2016. Internet Society.

Kastelic, A. 2015. International Law of State Responsibility: Unlawful Orchestration Versus the Omission of the Duty to Prevent the Unlawful Cyber Operations. COMPENDIUM. RACVIAC.

Best practices in cyber security from intergovernmental discussions, and a private sector proposal. 2017. Richard Hill, Hill & Associates.

Understanding Demand for Cyber Policy Resources. RTI report for the Hewlett Foundation's Cyber Initiative. 2017. Hewlett Foundation

International Cooperation Between CERTS: WS38 Technical Diplomacy for Cybersecurity. Panel discussion. 2017. Internet Governance Forum.

The IT industry's cybersecurity principles for industry and government. 2011. Information Technology Industry Council.

Industry Consortium for Advancement of Security on the Internet (ICASI).

Osula A.M. and Roigas, H. (eds.). 2016. International Cyber Norms: Legal, Policy & Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

Tallinn Manual on the international law applicable to cyber warfare. 2013. NATO Cooperative Cyber Defence Centre of Excellence.

Securing the Modern Economy: Transforming Cybersecurity Through Sustainability. 2018. Public Knowledge.

Stateless Attribution. Toward international accountability in cyberspace. 2017. RAND.

Farwell, J. 2012. Industry's vital role in national cyber security. Strategic Studies Quarterly. pp.10-41.

Finnemore, M. and Hollis, D. B. 2016. Constructing Norms for Global Cybersecurity. The American Journal of International Law. vol.110 no.3 pp.425-479.

Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience. 2012. World Economic Forum.

Global Agenda Council on Cybersecurity. White Paper. 2016. World Economic Forum.

Cyber Resilience. Playbook for Public-Private Cooperation. 2018. World Economic Forum.

Erice Declaration on Principles for Cyber Stability and Cyber Peace. 2009. World Federation of Scientist. 2009.