DiPLO
www.diplomacy.edu

Geneva Dialogue for Responsible Behaviour in Cyberspace

in the context of international peace and security

Baseline study

June 2019

Contents

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 on Responsible Behaviour in Cyberspace was initiated in spring 2018 and led by the Swiss FDFA, GIP, UNIDIR, ETH Zurich and the University of Lausanne. The aim of the dialogue was threefold: to analyze roles and responsibilities of various stakeholders in cyberspace, to provide a platform in Geneva for increased cooperation of existing stakeholders, and finally, to present recommendations on how these actors can cooperate as to contribute to greater stability and security in cyberspace.*

The Geneva Dialogue for Responsible Behaviour in Cyberspace aimed to do precisely this. By mapping the roles and obligations pertaining to responsible behaviour in cyberspace of different actor clusters, the project provided 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 document in front of you details the research process, the methodology used, as well as the preliminary clusters of actors and roles and obligations of actors in cyberspace. Furthermore, this paper deals with the explanation of the clusters of actors developed from within the stakeholder community, and it also entails 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.

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 users, 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 documents 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 that 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.

It is important to understand that there is no 'one-size fits all' approach as actor clusters, as well as actors within different clusters, vary in capacities and capabilities, understandings of cyberspace and approaches to peace and security, authority and legislative powers, and the degree to which they can influence and/or control the digital environment. As a result, actors assume, or are expected to assume, a variety of roles and responsibilities, depending on the context. Due to these differences, there is some overlap between the roles and responsibilities that are already assumed and those being suggested and advocated for, as actors within the same cluster vary in capability for their

implementation. Nevertheless, such repetitive patterns hint that there is already general broad agreement on the role and responsibilities that different actors should take.

What follows is the mapping for roles and responsibilities of each cluster of actors. For each cluster, first, the roles and responsibilities defined by the State actor cluster are outlined. These are divided into those already assumed, and those that are currently being promoted and/or advocated for. Second, the roles and responsibilities expected to be assumed by states by the remaining two actor clusters are also outlined.

Roles and Responsibilities of States

National governments do, or are expected to, act as stakeholders, regulators, coordinators, defenders, users, promoters and educators, while at the same time balancing aspects of cooperation, both international and multi-stakeholder.

Roles and Responsibilities defined by the State actor cluster

Assumed Roles and Responsibilities

The following roles and responsibilities have thus far been agreed by states in international and intergovernmental forums:

- Development and adoption of a cybersecurity framework. This role primarily falls into the scope of activities to be taken by states, that is, national governments. Developing a cybersecurity framework refers to establishing national cybersecurity policies that include legislative and procedural measures, define roles both of various government bodies as well as members of the wider stakeholder community, including identification of risks and critical infrastructure, adoption of strategies pertaining to legislative reform and development, capacity building and cooperation, and strategic approaches, as well as defining mutual assistance laws. More specifically listed responsibilities also include establishment of Computer Emergency Response Teams (CERTs) and National Points of Contact.[1]
- Awareness raising among the private sector and the general public, through capacity building in the form of promoting educational and training programmes on risks in cyberspace.[2]
- Capacity building nationally, as well as supporting that of other countries. This is (to be) done through training and education, engagement in public-private partnerships and international

[1] *African Union Convention on Cyber Security and Personal Data Protection*. 2014. African Union. *APEC Cybersecurity Strategy*. 2002. APEC. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation. *Commonwealth Cyber Declaration*. 2018. The Commonwealth. *NIS Directive*. 2016. European Union. *Declaration strengthening cyber-security in the Americas*. 2012. Organisation of American States. *Recommendations of the CICTE cybersecurity practitioners' workshop on OAS integral cybersecurity strategy: Framework for establishing the Inter-American CSIRT watch and warning network*. 2004. Organisation of American States. *Decision no.1106*. 2013. OSCE.

[2] *APEC Cybersecurity Strategy*. 2002. APEC. *Resolution 130*. 2014. ITU. *Recommendations of the CICTE cybersecurity practitioners' workshop on OAS integral cybersecurity strategy: Framework for establishing the Inter-American CSIRT watch and warning network*. 2004. Organisation of American States.

cooperation, primarily fostering digital literacy, but also enabling more effective international cooperation.[3]

- Cooperation, including international, intergovernmental and regional through the establishment of, and engagement in, public-private partnerships, transparency and information sharing. More specifically listed activities also include technical aspects of cooperation include joint incident response efforts, as well as development of a regional CERT.[4]
- Norm development, in terms of codes of practice, standards, confidence-building measures, and norms of responsible behaviour, through engagement in public-private partnerships and international cooperation. The latter are to be arrived at through stages, implementing CBMs and standards on interoperability, regional cooperation as well as definitions (terminology) first.[5]
- Development of, and engagement in, public-private partnerships by supporting the private sector, fostering PPP development and coordinating such partnerships. The purpose of such efforts is to enable capacity building, awareness raising and information sharing, as well as collective action contributing to general cybersecurity.[6]

---

[3] *APEC Cybersecurity Strategy*. 2002. APEC. *Dubai Action Plan 2015-2017*. 2015. Commonwealth of Independent States. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation. *Strategic Plan of the Commonwealth Telecommunications Organisation for the period 2016-2020*. 2016. Commonwealth Telecommunications Organisation. *Commonwealth Cyber Declaration*. 2018. The Commonwealth. *Resolution 130*. 2014. ITU.

[4] *African Union Convention on Cyber Security and Personal Data Protection*. 2014. African Union. *APEC Cybersecurity Strategy*. 2002. APEC. *APEC Telecom and Information Working Group. Strategic Action Plan 2016-2020*. 2015. APEC. *ASEAN Leaders' statement on cybersecurity cooperation*. 2018. ASEAN. *ASEAN ICT Master Plan 2020*. 2015. ASEAN. *Fortaleza Declaration*. 2014. BRICS. *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. 2017. European Union. *The principles and actions on cyber*. 2016. G7. *Antalya Summit Declaration*. 2015. G20. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation. *Commonwealth Cyber Declaration*. 2018. The Commonwealth. *Resolution 45*. 2014. ITU. *Resolution 50*. 2016. ITU. *Resolution 130*. 2014. ITU. *Decision no.1106*. 2013. OSCE. *Declaration strengthening cyber-security in the Americas*. 2012. Organisation of American States. *Adoption of a comprehensive Inter-American Strategy to combat threats to cybersecurity*. 2004. Organisation of American States.

[5] *APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice*. 2011. APEC. *ASEAN Regional Forum Work Plan on Security and the use of Information and Communication Technologies*. 2015. ASEAN. *ASEAN Leaders' statement on cybersecurity cooperation*. 2018. ASEAN. *ASEAN ICT Master Plan 2020*. 2015. ASEAN. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation. *Commonwealth Cyber Declaration*. 2018. The Commonwealth. *G7 Declaration on responsible states behaviour in cyberspace*. 2017. G7. *Progress update on Cyber Lexicon*. 2018. G20. *Resolution 45*. 2014. ITU. *Resolution 50*. 2016. ITU. *Resolution 130*. 2014. ITU. *NIS Directive*. 2016. European Union. *Establishment of a working group on cooperation and confidence-building measures in cyberspace*. 2017. Organisation of American States. *Adoption of a comprehensive Inter-American Strategy to combat threats to 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. *Decision no.1106*. 2013. OSCE.

[6] *African Union Convention on Cyber Security and Personal Data Protection*. 2014. African Union. *APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice*. 2011. APEC. *APEC Telecom and Information Working Group. Strategic Action Plan 2016-2020*. 2015. APEC. *ASEAN ICT Master Plan 2020*. 2015. ASEAN. *Dubai Action Plan 2015-2017*. 2015. Commonwealth of Independent States. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation. *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. 2017. European Union.

- Ensuring security of end-users and the wider national community, through establishing comprehensive and effective national cybersecurity frameworks, protection of critical infrastructure and engagement in public-private cooperation.[7]
- Responsible behaviour, as a responsibility of all actors in the stakeholder community, but primarily focused on states, sees agreements on taking responsibility for actions in cyberspace, considering the notion of human rights in terms of freedom of expression and privacy, respecting existing norms and confidence-building measures, engaging in international dialogue, and practicing restraint from threats of use of force. Negative responsibilities refer to agreements *not* to 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.[8]

Advocated Roles and Responsibilities

The following roles and responsibilities have thus far been proposed by states in international and intergovernmental forums:

- Adopting comprehensive national cybersecurity frameworks primarily through policy development and establishment of Computer Emergency Response Teams. Compliance programmes and procurement practices are also seen as an element of pressure for establishing a clear direction for other economies and social actors.[9] Comprehensive frameworks should have in place relevant mechanisms that include technical, policy-oriented, diplomatic and legislative measures.[10]
- Awareness raising among all stakeholders, through engagement in public-private partnerships.[11]
- Capacity building of developing countries and small and medium enterprises, through awareness raising and education.[12]
- Cooperation, fostered by public-private partnerships, information sharing, accountable behaviour and confidence-building measures, at the bilateral, regional and international level.[13]

---

[7] *Commonwealth Cybergovernance Model.* 2014. Commonwealth Telecommunications Organisation. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013. European Union. *G7 fundamental elements for effective assessment of cybersecurity in the financial sector*. 2016. G7. *Resolution 45*. 2014. ITU. *NATO Industry Cyber Partnership*. NATO CCD CoE. *Declaration strengthening cyber-security in the Americas*. 2012. Organisation of American States.

[8] *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation. *G7 Declaration on responsible states behaviour in cyberspace*. 2017. G7. *Antalya Summit Declaration*. 2015. G20.

[9] *The role and responsibilities of an effective regulator*. 2009. ITU. *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *Cybersecurity policy making at a turning point*. 2012. OECD. *Decision no.1106*. 2013. OSCE. *2015 GGE Report*. United Nations.

[10] *Chair's Statement*. 2015. Global Conference on Cyberspace.

[11] *The role and responsibilities of an effective regulator*. 2009. ITU. *2013 GGE Report*. United Nations.

[12] *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *The role and responsibilities of an effective regulator*. 2009. ITU. *International Code of Conduct for Information Security*. 2015. Shanghai Cooperation Organisation. *2013 GGE Report*. United Nations. *2015 GGE Report*. United Nations.

[13] *Chair's Statement*. 2015. Global Conference on Cyberspace. *The role and responsibilities of an effective regulator*. 2009. ITU. *Decision no.1202*. 2016. OSCE. *International Code of Conduct for Information Security*. 2015. Shanghai Cooperation Organisation. *Astana Declaration*. 2017. Shanghai Cooperation Organisation. *2015 GGE Report*. United Nations.

- Norm development through engagement in establishing standards and confidence-building measures, as well as engagement in public-private partnerships. Specifically, pressure that states can exert through procurement decisions are seen as potentially contributing to establishing norms referring to technologies but also legislative requirements.[14]
- Establishment of, and engagement in, public-private partnerships aimed at developing comprehensive cybersecurity frameworks, ensuring responsible behaviour of participating actors, protecting critical infrastructure, fostering international cooperation and providing for broad cybersecurity in general.[15]
- Ensuring overall national security.[16]
- Policy development that sets out the national cybersecurity framework, in consultation with other stakeholders through public-private partnerships.[17]
- Responsible behaviour through developing comprehensive cybersecurity frameworks that take into account questions of human rights, respect of existing norms and cooperation. Restraint is also seen as a key element of responsible behaviour, including restraint from threats, proliferation of malicious ICT tools and techniques and malicious international activities overall.[18] Transparency about the role and responsibilities of defence forces and security services in the cyber domain is also listed as a specific responsibility.[19] Negative responsibilities include preventive measures and ensuring states do *not* carry out activities that run counter to the task of maintaining international peace and security or have their territory used to launch attacks against other states.[20] Ensuring digital space is not used by terrorists and radical groups also falls in this category.[21] Freeing up cyberspace from government and commercial censorship is also listed here[22], as is ensuring equal access for all stakeholders.[23] A specific suggestion is to work on depoliticisation and desecuritisation of the role and work of Computer Emergency Response Teams[24], as well as ensuring civilian CERTs are by no means prevented to respond to incidents.[25]

---

[14] *Proposal for a Regulation of the EP and the Council on ENISA, the "EU Cybersecurity Agency"*. 2017. European Union. *The role and responsibilities of an effective regulator*. 2009. ITU. *Cybersecurity policy making at a turning point*. 2012. OECD. *International Code of Conduct for Information Security*. 2015. Shanghai Cooperation Organisation. *2010 GGE Report*. United Nations.

[15] *Commonwealth Cyber Declaration*. 2018. The Commonwealth. *Chair's Statement*. 2015. Global Conference on Cyberspace. *The role and responsibilities of an effective regulator*. 2009. ITU. *Decision no.1202*. 2016. OSCE. *International Code of Conduct for Information Security*. 2015. Shanghai Cooperation Organisation. *2015 GGE Report*. United Nations.

[16] *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *2015 GGE Report*. United Nations.

[17] *The role and responsibilities of an effective regulator*. 2009. ITU. *Cybersecurity policy making at a turning point*. 2012. OECD.

[18] *Chair's Statement*. 2011. Global Conference on Cyberspace. *Chair's Statement*. 2015. Global Conference on Cyberspace. *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *2015 GGE Report*. United Nations.

[19] *Chair's Statement*. 2015. Global Conference on Cyberspace.

[20] *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *International Code of Conduct for Information Security*. 2015. Shanghai Cooperation Organisation. *Report of the International Security Cyber Issues Workshop Series*. 2016. UNIDIR. *2015 GGE Report*. United Nations.

[21] *Chair's Statement*. 2017. Global Conference on Cyberspace.

[22] *Chair's Statement*. 2011. Global Conference on Cyberspace.

[23] *Chair's Statement*. 2015. Global Conference on Cyberspace.

[24] *Voluntary, non-binding norms for responsible state behaviour in the use of information communications technology*. 2017. UNODA.

[25] *Chair's Statement*. 2015. Global Conference on Cyberspace.

One specific suggestion includes having States encouraging additional analysis and study by research institutes and universities on matters of ICT security. Here, States are encouraged to consider what role UN research and training institutes could play in this regard.[26]

Roles and Responsibilities of States suggested by other actor clusters

The private sector has thus far argued that states should, among other, bear the responsibility of:

- Adopting national cybersecurity frameworks that define National Points of Contact.[27]
- Norm development through standardisation and international cooperation.[28]
- Development of, and engagement in, public-private partnerships to ensure balanced policy development.[29]
- Ensure security through engagement in public-private partnerships, addressing the security of people, businesses and infrastructures, building a reliable basis for trust.[30]
- Responsible behaviour based on transparency, taking into account human rights, primarily baseline privacy principles. Restraint is a core element, referring to refraining from threats, pressure and attacks on the private sector and critical infrastructures, and cyber weapons development.[31]

The communities and users have thus far argued that states should, among other, bear the responsibility of:

- Adopting comprehensive national cybersecurity frameworks, through policy development and engagement in public-private partnerships.[32]
- Awareness raising among the general public.[33]
- Capacity building of the state actor cluster in order to be able to develop baseline capacity levels to participate in the development and implement agreed confidence-building measures.[34]
- Cooperation, namely international, through state-to-state contracts, bilateral cyber pacts and international for a, primarily in the form of information sharing, but also technical cooperation through provision of assistance.[35]

---

[26] *2013 GGE Report*. United Nations.

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

[28] *Cybersecurity policy making at a turning point*. 2012. OECD.

[29] *Cybersecurity policy making at a turning point*. 2012. OECD.

[30] *Digital Security and Due Process: Modernising cross-border government access standards for the cloud era*. 2017. Google. *International Cybersecurity Norms*. 2016. Microsoft. *The need for a Digital Geneva Convention*. 2017. Microsoft. *Charter of Trust. For a secure digital world*. 2018. Siemens.

[31] *The need for a Digital Geneva Convention*. 2017. Microsoft. *International Cybersecurity Norms*. 2016. Microsoft. *From Articulation to Implementation: Enabling progress on cybersecurity norms*. 2016. Microsoft.

[32] *Getting beyond norms. New approaches to international cyber security challenges*. 2017. CIGI. *Multi-stakeholderism: Anatomy of an inchoate global institution*. 2016. GCIG. *Delhi Communique on a GFCE global agenda for cyber capacity building*. 2017. GFCE. *Global Agenda Council on Cybersecurity*. 2016. WEF.

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

[34] *International Cyber Norms*. 2016. Osula & Roigas (eds.). NATO CCD CoE.

[35] *Confidence-building measures in cyberspace*. 2014. Atlantic Council. *Rights and Responsibilities in Cyberspace*. 2010. East-West Institute. *Briefings from the Research Advisory Group*. 2017. GCSC. *The IT industry's cybersecurity principles for industry and government*. 2011. Information Technology Industry Council.

- Norm development through engaging in standard development, establishment of codes of conduct and a harmonised global legal framework to take into account procedural provisions regarding assistance. On the technical side, states are seen as having a role in foster the development of open standards and permission-less innovation for security solutions. A specific suggestion sees states 'leading by example' in procurement decisions, pushing thus for standards in product development.[36] A step further includes the suggestion of establishing an international cyberattack attribution organisation, with the aim of strengthening trust online.[37]
- Establishment of, and engagement in, public-private partnerships through facilitation of such frameworks in the first place. These are then to be used for capacity building, information sharing and as frameworks for international cooperation.[38]
- Ensuring security adopting comprehensive approaches, by ensuring, primarily, national security, acting on intelligence obtained, regulating private sector activities through national cybersecurity frameworks and engaging in public-private and international cooperation.[39]
- Responsible behaviour by assuming responsibility for attributable cyber operations. Specifically, states are seen as actors expected to assume the majority of negative responsibilities, in terms of ensuring that cyberspace is *not* used for any form of exploitation, that security of the private sector is *not* undermined, nor public trust in the internet, and that they themselves do *not* conduct any activities that would damage the stability of cyberspace.[40] Restraint from hacking personal accounts or private data, using ICTs to steal intellectual

International Cyber Norms. 2016. Osula & Roigas (eds.). NATO CCD CoE. Hill, R. 2018. *Best practices in cyber security from intergovernmental discussions, and a private sector proposal*. 2017. Richard Hill, Hill & Associates. *Risk and Responsibility in a Hyperconnected World*. 2012. WEF.

[36] *Constructing Norms for Global Cybersecurity*. 2016. Finnemore and Hollis. *Delhi Communique on a GFCE global agenda for cyber capacity building*. 2017. GFCE. *Cybersecurity policy making at a turning point*. 2012. OECD. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge. *Global Agenda Council on Cybersecurity*. 2016. WEF. *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. 2009. World Federation of Scientists.

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

[38] *Breaking the Cyber-Sharing Logjam*. 2015. Atlantic Council. *Confidence-building measures in cyberspace*. 2014. Atlantic Council. *The Proposed Digital Geneva Convention: Towards an inclusive public-private agreement on cyberspace?* 2017. GCSP. *International Cyber Norms*. 2016. Osula & Roigas (eds.). NATO CCD CoE. *Cybersecurity policy making at a turning point*. 2012. OECD. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge. *Best practices in cyber security from intergovernmental discussions, and a private sector proposal*. 2017. Richard Hill, Hill & Associates. *Risk and Responsibility in a Hyperconnected World*. 2012. WEF.

[39] *Rights and Responsibilities in Cyberspace*. 2010. East-West Institute. *Industry's vital role in national cyber security*. 2012. Farewell. *Good neighbours make good security: Coordinating EU critical infrastructure protection against cyber threats*. 2017. GLOBSEC. A. Kastelic. 2015. *International Law as State Responsibility*. RACVIAC. *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF. *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. 2009. World Federation of Scientists.

[40] *Getting Beyond Norms. New approaches to international cyber security challenges*. 2017. CIGI. *Call to Protect the Public Core of the Internet*. 2017. GCSC. A. Kastelic. 2015. *International Law as State Responsibility*. RACVIAC. *Tallinn Manual*. 2013. NATO CCD CoE. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge. *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. 2009. World Federation of Scientists.

property or requiring 'backdoors' in mass-market commercial technology products is also included in this cluster.[41]

In terms of state activities already taking place, civil society actors recognise that states already engage in security provision through fostering national defence and resilience.[42] Efforts aimed at norm development are also recognised, practiced through activities aimed at standards development.[43] Finally, state efforts aimed at adopting comprehensive national cybersecurity frameworks through public-private cooperation are also referred to as already ongoing activities.[44]

Roles and Responsibilities of the Private Sector

Private enterprise and corporations do, or are expected to, act as stakeholders, service providers, defenders, coordinators and promoters of cybersecurity, while at the same time balancing between government regulation and end-user demands, as well as different aspects of cooperation they engage in, both international and multi-stakeholder.

Roles and Responsibilities defined by the Private Sector cluster

Assumed Roles and Responsibilities

The following roles and responsibilities have thus far been agreed by the private sector in developed initiatives and attempts at self-regulation:

- Awareness raising among the wider pool of end-users and the developer community on threats and protection methods. Special focus of some initiatives is placed on the Internet of Things (IoT).[45]
- Capacity building of the private sector and the general public through education and engagement in public-private partnerships.[46]
- Cooperation through information sharing on best practice and vulnerabilities.[47]
- Norm development for the industry through standardisation, focused on software assurance and secure development practices ('security by design' standards).[48]
- Ensuring security of end-users, primarily through 'security by design' principles, prioritising security, privacy, integrity and reliability.[49]

---

[41] *Best practices in cyber security from intergovernmental discussions, and a private sector proposal*. 2017. Richard Hill, Hill & Associates.
[42] *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.
[43] *G7 fundamental elements for effective assessment of cybersecurity in the financial sector*. 2016. G7. *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.
[44] *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.
[45] *IoT Cybersecurity Alliance*. 2017. AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic. *Cybersecurity Tech Accord*. 2018. Microsoft.
[46] *IoT Cybersecurity Alliance*. 2017. AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic. *Cybersecurity Tech Accord*. 2018. Microsoft.
[47] *Initiative explanation*. Industry Consortium for Advancement of Security in the Internet.
[48] *Initiative explanation*. Industry Consortium for Advancement of Security in the Internet. *SAFECode Fundamental Practices for Secure Software Development*. 2018. SAFECode.
[49] *Cybersecurity Tech Accord*. 2018. Microsoft.

- Responsible behaviour, namely through transparency. Recent examples include pledges to inform users of potential account attacks and breaches by suspected state-sponsored actors. Negative responsibilities of the private sector refer to agreements *not* to aid governments in launching cyberattacks.[50]

Advocated Roles and Responsibilities

The following roles and responsibilities have thus far been proposed by the private sector in developed initiatives and attempts at self-regulation:

- Cooperation at the international level, primarily through information sharing on incidents, as well as coordination of vulnerability responses.[51]
- Norm development through development of shared principles and standards aimed at self-regulation.[52]
- Engagement in public-private partnerships aimed at providing cybersecurity through provision of support to authorities, incident response and policy input.[53]
- Ensure security, both own and that of end-users, through abiding by 'security by design' principles, including products, functionalities, processes, technologies, operations, architectures, and business models, as well as standardisation and engagement in public-private cooperation.[54]
- Policy development in terms of providing policy input and technical expertise to make policies developed feasible.[55]
- Responsible behaviour through practicing restraint by limiting support to governments to genuinely defensive scenarios.[56] Suggested negative responsibilities relate to *not* aiding attacks on end-users anywhere.[57]

Roles and Responsibilities of the Private Sector suggested by other actor clusters

States have thus far argued that the private sector should, among other, bear the responsibility of:

[50] *Notification for targeted attacks*. 2015. Facebook. *Security warnings for suspected state-sponsored attacks*. 2012. Google. *Cybersecurity Tech Accord*. 2018. Microsoft. *Additional steps to help keep your personal information secure*. 2015. Microsoft. *Yahoo to notify its users about 'state-sponsored' hacking attacks*. 2015. Guardian.

[51] *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. *Charter of Trust. For a secure digital world*. 2018. Siemens.

[52] *The need for a Digital Geneva Convention*. 2017. Microsoft.

[53] *International Cybersecurity Norms*. 2016. Microsoft. *Charter of Trust. For a secure digital world*. 2018. Siemens.

[54] *International Cybersecurity Norms*. 2016. Microsoft. *The need for a Digital Geneva Convention*. 2017. Microsoft. *From Articulation to Implementation: Enabling progress on cybersecurity norms*. 2016. Microsoft. *Charter of Trust. For a secure digital world*. 2018. Siemens.

[55] *From Articulation to Implementation: Enabling progress on cybersecurity norms*. 2016. Microsoft. *International Cybersecurity Norms*. 2016. Microsoft. *Charter of Trust. For a secure digital world*. 2018. Siemens.

[56] *From Articulation to Implementation: Enabling progress on cybersecurity norms*. 2016. Microsoft.

[57] *The need for a Digital Geneva Convention*. 2017. Microsoft.

- Capacity building through training and education of technology security experts, as well as bolstering the capacities of small and medium enterprise and individuals.[58]
- Norm development through developing codes of practice by 'peak industry groups' as well as technical standards to protect security.[59]
- Ensuring security, primarily its own, through capacity building and adopting adequate levels of cybersecurity safeguards in business practice, including adoption of 'security by design' principles[60], as well as through engagement in public-private partnerships[61].
- Responsible behaviour, ensuring that security measures included in ICT products and services do not undermine human rights, abiding also by principles of transparency and accountability accordingly.[62]

Expert communities and users have thus far argued that the private sector should, among other, bear the responsibility of:

- Adopting a cybersecurity framework, developing policies based on existing legislation.[63]
- Capacity building of the workforce through education.[64]
- Cooperation through information sharing, establishing potentially a formal legal regime[65] but primarily assist public sector efforts to proactively defend against cyberattacks and minimise the duration and impact of such attacks[66].
- Norm development, as a bottom-up approach, primarily through standardisation.[67]
- Ensuring security, primarily their own, though acting on intelligence obtained, correcting software vulnerabilities, adopting 'security by design' principles and encryption.[68] Seen as providing the first line of security by some actors[69], the private sector is further expected to engage in information sharing and threat awareness to fulfil this role, responsibly developing

[58] *APEC Cybersecurity Strategy*. 2002. APEC. *Digital security risk management for Economic and Social Prosperity*. 2015. OECD.
[59] *APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice*. 2011. APEC. *The role and responsibilities of an effective regulator*. 2009. ITU.
[60] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013. European Union. *Chair's Statement*. 2015. Global Conference on Cyberspace. *The role and responsibilities of an effective regulator*. 2009. ITU. *Digital security risk management for Economic and Social Prosperity*. 2015. OECD.
[61] *Chair's Statement*. 2011. Global Conference on Cyberspace.
[62] *Cybersecurity Strategy of the European Union: AN Open, Safe and Secure Cyberspace*. 2013. European Union. *Digital security risk management for Economic and Social Prosperity*. 2015. OECD.
[63] *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge.
[64] *Ibid*.
[65] *Exploring Multi-Stakeholder Internet Governance*. 2015. East-West Institute. *The proposed Digital Geneva Convention: Towards an inclusive public-private agreement on cyberspace?* 2017. GCSP. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge.
[66] *Best practices in cyber security from intergovernmental discussions, and a private sector proposal*. 2017. Richard Hill, Hill & Associates.
[67] *The proposed Digital Geneva Convention: Towards an inclusive public-private agreement on cyberspace? 2017.* GCSP. *The IT industry's cybersecurity principles for industry and government*. 2011. Information Technology Industry Council. *International Cyber Norms*. 2016. Osula & Roigas (eds.). NATO CCD CoE. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge. *Global Agenda Council on Cybersecurity*. 2016. WEF.
[68] *Global Internet Report*. 2016. ISOC.
[69] *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.

patch management processes and keeping software up to date.[70] One specific claims that private sector actors are better positioned than most national governments to develop real-time threat awareness, contributing thus to the maintenance of cyber defence postures.[71]

- Responsible behaviour mainly in term of negative responsibilities of *not* engaging in activities damaging the stability of cyberspace, trafficking in cyber vulnerabilities for offensive purposes, attacking the information infrastructure or exploiting users.[72] Optimisation of data collected is also seen as an element of responsible behaviour.[73] A specific task attributed to the private sector is to also ensure that the role of Computer Emergency Response Teams is by no means politicised.[74]

Additionally, academic actors have suggested that private sector should develop public-private partnerships enabling this actor cluster to gain access to the experience it lacks and develop better comprehension of its own responsibilities.[75] Namely, cybersecurity is highlighted as a shared responsibility and it is stressed that the private sector should not expect states to do 'all the heavy lifting'.

Civil society actors have also recognised that the private sector has thus far already engaged in norm development through promoting standards as well as general efforts aimed policy development through provision of policy input and technical expertise.[76] In terms of responsible behaviour, the role the private sector plays in matters related to human rights has also been recognised, especially in light of political instability, as well as the growing trend of bug-bounty programmes developed by this actor cluster, aimed at finding existing vulnerabilities.[77]

Roles and Responsibilities of Communities and Users

When it comes to communities and users, its members do, or are expected to, act as stakeholders, defenders, users, promoters, researchers and educators, encompassing a wide array of diverse actors, while at the same time balancing aspects of cooperation, both international and multi-stakeholder.

---

[70] *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*. 2016. GCIG. *Getting beyond norms. New approaches to international cyber security challenges*. 2017. CIGI. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge. *Best practices in cyber security from intergovernmental discussions, and a private sector proposal*. 2017. Richard Hill, Hill & Associates. *Global Agenda Council on Cybersecurity*. 2016. WEF. *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF. *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. 2009. World Federation of Scientists.

[71] *International Cyber Norms*. Osula & Roigas (eds.). NATO CCD CoE.

[72] *Call to Protect the Public Core of the Internet*. 2017. GCSC. *Best practices in cyber security from intergovernmental discussions, and a private sector proposal*. 2017. Richard Hill, Hill & Associates. *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. 2009. World Federation of Scientists.

[73] *Global Internet Report*. 2016. ISOC.

[74] *International Cooperation Between CERTs: WS38 Technical Diplomacy for Cybersecurity*. Panel presentation: Van Horenbeeck. 2017. IGF.

[75] *Industry's vital role in national cyber security*. 2012. Farwell.

[76] *International Cyber Norms*. 2016. Osula & Roigas (eds.). NATO CCD CoE. *Understanding Demand for Cyber Policy Resources*. 2017. RTI Report for Hewlett Foundation. *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.

[77] *UN cyberspace and international peace and security*. 2017. UNIDIR. *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.

Roles and Responsibilities defined by the Communities and Users cluster

Assumed Roles and Responsibilities

The following roles and responsibilities have thus far been agreed communities and users in developed initiatives:

- Capacity building for organisation focused on internal cyber capabilities and resilience.[78]

In terms of roles already assumed and implemented, this actors cluster recognises the following:

- Norm development through engagement of Centres of Excellence in cyber norms discussion.[79]
- Engagement of communities and users in public-private partnerships aimed at policy development.[80]
- Policy development through provision of policy input and expertise.[81]

Advocated Roles and Responsibilities

The following roles and responsibilities have thus far been proposed by communities and users in developed initiatives:

- Awareness raising among the general public through education, supporting end-users in maintaining own cybersecurity and making informed purchasing decisions.[82]
- Capacity building of civil society actors, through education.[83]
- Cooperation at the international level. The expert community particularly encourages CERTs to continue establishing own patterns of interaction and rules of procedure, developing own channels of communication to manage everyday incidents.[84]
- Norms development whereby the technical community focuses on establishing technical standards, while civil society organisations mainly advocate for developing confidence-building measures, as well as pressure for 'security by design' principles exerted through procurement decisions of actors within this cluster.[85]
- Ensure security, primarily their own, through abiding by internationally accepted best practices and standards and utilizing privacy and security technologies.[86] End-users are seen

[78] *Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience*. 2012. WEF.
[79] *International Cyber Norms*. 2016. Osula & Roigas (eds.). NATO CCD CoE.
[80] *Understanding Demand for Cyber Policy Resources*. 2017. RTI Report for Hewlett Foundation.
[81] *Ibid*.
[82] *Global Agenda Council on Cybersecurity*. 2016. WEF.
[83] *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge.
[84] *International Cooperation Between CERTs: WS38 Technical Diplomacy for Cybersecurity.* Panel presentation: Carr. 2017. IGF. *International Cooperation Between CERTs: WS38 Technical Diplomacy for Cybersecurity*. Panel presentation: Geiger. 2017. IGF.
[85] *Confidence-building measures in cyberspace*. 2014. Atlantic Council. Initiative explanation. *CEN-CENELEC Focus Group on Cybersecurity*. *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*. 2016. GCIG. *The IT industry's cybersecurity principles for industry and government*. 2011. Information Technology Industry Council. *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge.
[86] *Securing the Modern Economy: Transforming Cyber Security Through Sustainability*. 2018. Public Knowledge. *Erice Declaration on Principles for Cyber Stability and Cyber Peace*. 2009. World Federation of Scientists.

as bearing the responsibility of practicing good cyber hygiene and managing software patches.[87] One specific view advocates for cyberspace policy experts, legal scholars, and international policy experts from a diversity of academia and research organizations, joining forces with private sector actors in attributing cyberattacks, since the private sector and the technical community are seen as possessing sufficient capacity and expertise.[88] This view sees the state playing a secondary role in this process. Finally, non-governmental CERTs are highlighted as the most direct form of this actor cluster's involvement in security provision.[89]

- Policy development through provision of policy input and independent advice.[90] Participation in the policy development process can be ensured through direct or indirect lobbying efforts. Working closely with academia and the private sector to provide evidence-based research is seen as a starting point for such efforts.[91]
- Responsible behaviour, seeing end-users assuming own responsibility for their digital security. negative responsibilities refer to *not* engaging in activities that potentially damage the stability of cyberspace.[92]

A specific role that is suggested within the research sample poses as an outlier and is one of having civil society organisations acting as a watchdog for government policies, specifically in terms of monitoring budget spending and industry practices. CSOs are seen as further capable of developing and promoting standards for transparency reporting on cyber security issues.[93]

Roles and Responsibilities of Communities and Users suggested by other actor clusters

States have thus far argued that the broader civil society community should, among other, bear the responsibility of:

- Ensuring security, their own[94], as well as that of end-users of installing technical safeguards for the ICTs they use.[95] Cooperation among ethical hackers and the wider ICT community is also seen as an important model contributing to security.[96]
- Policy development through provision of policy input advocating for a comprehensive approach encompassing all actors in the stakeholder community.[97]
- Responsible behaviour, mainly in terms of having all end-users meeting minimum cyber hygiene requirements.[98]

---

87 *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*. 2016. GCIG.
88 *Stateless Attribution. Toward international accountability in cyberspace*. 2017. RAND.
89 *A Role for Civil Society?* 2014. ICT4Peace.
90 *Cybersecurity policy making at a turning point*. 2012. OECD.
91 A Role for Civil Society? 2014. ICT4Peace.
92 *Call to Protect the Public Core of the Internet*. 2017. GCSC.
93 *A Role for Civil Society?* 2014. ICT4Peace.
94 *Chair's Statement*. 2015. Global Conference on Cyberspace.
95 *The role and responsibilities of an effective regulator*. 2009. ITU.
96 *Chair's Statement*. 2015. Global Conference on Cyberspace.
97 *The role and responsibilities of an effective regulator*. 2009. ITU.
98 *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation.

A recognition of the actor cluster already engaging in ensuring security through multi-stakeholder cooperation has already been made.[99]

[99] *Chair's Statement*. 2015. Global Conference on Cyberspace.

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..*'[100]

Asia Pacific Economic Cooperation: '*..outreach to economies, industry and consumers regarding cybersecurity and cyberethics should be conducted..*'[101]

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..*'[102]

Asia Pacific Economic Cooperation: '*..engage governments, the private sector, other..*'[103]

Association of Southeast Asian Nations: '*..policy officials, diplomats, prosecutors as well as technical operators and analysts. It expects involvement of industry, NGOs and academia..*'[104]

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 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..*'[105]

Commonwealth: '*..appropriate consultative processes involving industry, academia, governments and other relevant stakeholders..*'[106]

Commonwealth: '*..[member countries will] working with relevant international organisations, the private sector, academic institutions, Commonwealth initiatives and their shareholders..*'[107]

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..*'[108]

Commonwealth Telecommunications Organisation: '*..governments, industry, civil society and users have a shared responsibility..*'[109]

---

[100] African Union Convention on Cyber Security and Personal Data Protection. 2014. African Union.
[101] APEC Cybersecurity Strategy. 2002. Asia Pacific Economic Cooperation.
[102] APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice. 2011. Asia Pacific Economic Cooperation.
[103] APEC Telecom and Information Working Group. Strategic Action Plan 2016-2020. 2015. Asia Pacific Economic Cooperation.
[104] ASEAN Cyber Capacity Programme. 2016. Association of Southeast Asian Nations.
[105] 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.
[106] Commonwealth Cyber Declaration. 2018. The Commonwealth.
[107] Ibid.
[108] Commonwealth approach for developing national cybersecurity strategies. 2015. Commonwealth Telecommunications Organisation.
[109] Commonwealth Cybergovernance Model. Commonwealth ICT Ministers forum 2014. Commonwealth Telecommunications Organisation. 2014.

European Union: '*..bring together the European External Action Service (EEAS), Member States' cyber authorities, EU agencies, Commission services, academia and civil society..*'[110]

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..*'[111]

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..*'[112]

International Telecommunications Union: '*..invites Member States, Sector Members, Associates and Academia..*'[113]

International Telecommunications Union: '*..encouraging academia to provide for the education.. […] ..allowing governments, businesses, civil society and individual users to work together..*'[114]

Organisation of American States: '*..promoting public sector cooperation with the private sector and academia..*'[115]

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..*'[116]

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..*'[117]

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..*'[118]

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*

[110] 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.

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

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

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

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

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

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

[117] 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.

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

identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations..'[119]

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..'*[120]

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..'*[121]

Broader civil society

Atlantic Council: '*..States are not the only […] actors in cyberspace.. […] ..role of companies, nongovernmental organizations, civil society, and others..'*[122]

Global Commission on Internet Governance: '*..four classes of actors: states, formal intergovernmental organizations (IGOs), firms and civil society actors..'*[123]

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..'*[124]

Global Forum on Cyber Expertise: '*..including governments, international organisations, private companies, civil society, technical community and academia..'*[125]

World Federation of Scientists: '*..governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs..'*[126]

World Economic Forum: '*..public-private partnerships [of the Government] with civil society and academia can also help..'*[127]

---

[119] 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.

[120] International Cybersecurity Norms. 2016. Microsoft.

[121] A Tech Accord to protect people in cyberspace. 2018. Microsoft.

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

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

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

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

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

[127] 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	"*..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

	capabilities for implementing standards and norms for cybersecurity and responsible behaviour in cyberspace	
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	*"..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

	behaviour of the actors involved	
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	"*..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

	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	"*..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.

Executive summary

The analytical basis of the Geneva dialogue, the study that was presented in May 2018 by DiploFoundation, provides insight into the roles and responsibilities of states, private sector actors, as well as communities and individuals in cyberspace, in the context of international peace and security. By analysing existing documents pertaining to responsible behaviour in cyberspace, the study identified possible roles and responsibilities of states, private sector, and communities and users.

The aim of the study was to present a comprehensive framework for the roles that belong to the specific actors in cyberspace, as well as those roles they should assume. To achieve this aim, various actors in cybersecurity were classified into three clusters, based on existing policy documents and frameworks, as well as initiatives, proposals, programmes, etc., developed by international and intergovernmental organisations, private enterprise and corporations, the technical and academic community, think-tanks and civil society organisations. The classification was achieved by employing qualitative content analysis on more than 70 documents. Based on the analysis, the team at DiploFoundation was able to map 280 roles and responsibilities overall.

For identifying attributed roles and responsibilities pertaining to state behaviour in cyberspace, official documents belonging to regional, intergovernmental and international organisations were analysed, e.g. APEC, ASEAN, EU, NATO, G7, OAS, OSCE, OECD, UN GGE, etc. In terms of identification of private sector actors' roles and responsibilities in cyberspace, Microsoft's proposals were mainly analysed, due to the fact that the company is most active in advocacy for cyberspace regulation. Additionally, documents belonging to Google, Facebook, Siemens, IoT Security Alliance, etc. were analysed. Finally, the broader civil society has also been active in promoting cooperation and regulation in cyberspace, which is why documents belonging to the following actors were also examined for the purpose of this study: Atlantic Council, Global Commission on Internet Governance, Global Commission on the Stability of Cyberspace, Global Forum on Cyber Expertise, World Federation of Scientists, World Economic Forum, etc.

The three broad categories of stakeholders that were identified in the study were states, private sector actors, and a general group of actors defined as communities and users. Whilst analysing roles and responsibilities of states in cyberspace, emphasis was put on states' behaviour and cooperation within regional, intergovernmental and international organisations and regimes. Regarding private sector actors, namely corporations and enterprises, research was conducted on cybersecurity-related documents on regional and international levels, as well as initiatives regarding self-regulation. Finally, the third cluster, defined as communities and individuals, consists of diverse actors such as the expert, technical community and associations, think-tanks, foundations and civil society organisations, as well as the academic sector.

Additionally, public-private partnership (PPP) initiatives were also analysed, as a direct form of cooperation between the first two clusters of the study. The unique position of national and supranational Computer Emergency Response Teams (CERTs) was also explored, seeing that their roles and responsibilities could belong to all three of the clusters of the study. Although CERTs can be associated with having the role of independent technical bodies, their activities can also be employed for political and diplomatic purposes, as well as bodies that assist in commercial endeavours, e.g. for media and non-governmental organisations.

Through analysing various documents pertaining to actor behaviour in cyberspace, the team at DiploFoundation decided to classify the roles and responsibilities into three categories: attributed, assumed and proposed roles and responsibilities.

During the analysis, an important differentiation was made: roles and responsibilities stemming from the actor cluster that are identified for the actor itself and those expected to be assumed by the actor by the actors belonging to the other two clusters that were analysed.