Roles and Responsibilities of the Private Sector

Geneva Dialogue for Responsible Behaviour in Cyberspace in the context of international peace and security

Introduction

This baseline study is one of three documents developed to serve as a basis for an inclusive dialogue among cybersecurity stakeholders on the specific roles and responsibilities to be embraced by the three identified strands of actors – the state, the private sector and communities and users. The clusters of roles and responsibilities presented within this baseline document 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 clearly made. For more details on the research process and development of these clusters, please consult the Research introductory document enclosed.

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, understanding 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 different actors should take. When it comes to 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.

Fostering a basis for developing stability and security of cyberspace therefore requires adopting new, *blended governance* approaches. The primary aim of these baseline studies developed is precisely to spark discussion on such approaches among key cybersecurity stakeholders, developing into a more comprehensive framework of international, multi-stakeholder dialogue on responsible behaviour in cyberspace.

The structure of this document is as follows. First, the roles and responsibilities defined by the Private Sector 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 the private sector by the remaining two actor clusters – states and communities and users –

are also outlined. These lists form the core of the baseline study. They are complemented by additional questions for consideration that arose during the initial research process for the purpose of this project. These have been selected based on their difference from the general patterns mapped and/or the unique approaches and solutions they suggest.

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).[1]
- Capacity building of the private sector and the general public through education and engagement in public-private partnerships.[2]
- Cooperation through information sharing on best practice and vulnerabilities.[3]
- Norm development for the industry through standardisation, focused on software assurance and secure development practices ('security by design' standards).[4]
- Ensuring security of end-users, primarily through 'security by design' principles, prioritising security, privacy, integrity and reliability.[5]
- 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.[6]

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:

[1] *IoT Cybersecurity Alliance*. 2017. AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic. *Cybersecurity Tech Accord*. 2018. Microsoft.
[2] *IoT Cybersecurity Alliance*. 2017. AT&T, IBM, Nokia, Palo Alto Networks, Symantec and Trustonic. *Cybersecurity Tech Accord*. 2018. Microsoft.
[3] *Initiative explanation*. Industry Consortium for Advancement of Security in the Internet.
[4] *Initiative explanation*. Industry Consortium for Advancement of Security in the Internet. *SAFECode Fundamental Practices for Secure Software Development*. 2018. SAFECode.
[5] *Cybersecurity Tech Accord*. 2018. Microsoft.
[6] *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.

- Cooperation at the international level, primarily through information sharing on incidents, as well as coordination of vulnerability responses.[7]
- Norm development through development of shared principles and standards aimed at self-regulation.[8]
- Engagement in public-private partnerships aimed at providing cybersecurity through provision of support to authorities, incident response and policy input.[9]
- 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.[10]
- Policy development in terms of providing policy input and technical expertise to make policies developed feasible.[11]
- Responsible behaviour through practicing restraint by limiting support to governments to genuinely defensive scenarios.[12] Suggested negative responsibilities relate to *not* aiding attacks on end-users anywhere.[13]

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:

- Capacity building through training and education of technology security experts, as well as bolstering the capacities of small and medium enterprise and individuals.[14]
- Norm development through developing codes of practice by 'peak industry groups' as well as technical standards to protect security.[15]
- 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[16], as well as through engagement in public-private partnerships[17].

---

[7] *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.

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

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

[10] *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.

[11] *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.

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

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

[14] *APEC Cybersecurity Strategy*. 2002. APEC. *Digital security risk management for Economic and Social Prosperity*. 2015. OECD.

[15] *APEC Guidelines for Creating Voluntary Cyber Security. ISP Codes of Practice*. 2011. APEC. *The role and responsibilities of an effective regulator*. 2009. ITU.

[16] *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.

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

- 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.[18]

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.[19]
- Capacity building of the workforce through education.[20]
- Cooperation through information sharing, establishing potentially a formal legal regime[21] but primarily assist public sector efforts to proactively defend against cyberattacks and minimise the duration and impact of such attacks[22].
- Norm development, as a bottom-up approach, primarily through standardisation.[23]
- Ensuring security, primarily their own, though acting on intelligence obtained, correcting software vulnerabilities, adopting 'security by design' principles and encryption.[24] Seen as providing the first line of security by some actors[25], the private sector is further expected to engage in information sharing and threat awareness to fulfil this role, responsibly developing patch management processes and keeping software up to date.[26] 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.[27]
- 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,

---

[18] *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.

[19] *Securing the Modern Economy: Transforming Cybersecurity Through Sustainability*. 2018. Public Knowledge.

[20] *Ibid*.

[21] *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.

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

[23] *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.

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

[25] *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.

[26] *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.

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

attacking the information infrastructure or exploiting users.[28] Optimisation of data collected is also seen as an element of responsible behaviour.[29] 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.[30]

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.[31] 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.[32] 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.[33]

Further questions for consideration

How much control do states have over the private sector in efforts to ensure cybersecurity?

Companies are seen as sometimes balancing minimal security measures against satisfying shareholder interests by maximising company profits, viewing cyber-threats as a tolerable risk. How necessary is it for governments to introduce measures that can potentially be seen as burdening for the private sector, compelling private actors to prioritise cybersecurity?[34]

Where do Computer Emergency Response Teams fit in the wider cybersecurity stakeholder landscape?

Even national Computer Emergency Response Teams 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. Should Computer Emergency Response Teams be allowed to operate as independent bodies engaged in

---

[28] *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.

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

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

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

[32] *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.

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

[34] *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.

cross-border technical communication and cooperation, or should they be politicised and used as part of the 'diplomatic toolkit' of states?[35]

Should the state have a greater role in private sector claims of attribution?

A greater role for the government in responding to private sector claims of attribution has been argued as potentially increasing accountability. The government's heightened responsibility would, in this view, increase its own accountability, as well as that of the private sector, through scrutiny of its attribution claim. Should the state have a greater role in private sector claims of attribution and what effect could this potentially have on the private sector in return?[36]

Can national normative frameworks socialise norms at the international level?

Even among like-minded countries, understandings and approaches to issues such as cybersecurity or human rights such as privacy vary, despite the fact that end-users' expectations generally do not. National legislative frameworks that have cross-border effects on the other hand necessitate changes in domestic normative frameworks of other countries – an example being EU's General Data Protection Regulation. How effectively can national normative frameworks push for adoption of principles and standards on a wider international scale, ultimately establishing specific patterns and norms of behavior?[37]

Can an international mechanism for attribution be established?

There have been suggestions that an international mechanism for attribution can be established based on operating principles to those of the International Atomic Energy Agency (IAEA). Namely, such a mechanism would enable governments and the private sector to provide evidence to support technical attribution and obtain some level of validation through rigorous peer review. Consisting of technical experts from across governments, the private sector, academia, and civil society with the capability to examine tactics, techniques, and procedures used by nation-state attackers, as well as indicators of compromise that suggest a given attack was by a nation-state, the mechanism would adopt decisions based on consensus. Its essential output would be a technical analysis of the attack and evidence of attribution.[38]

---

[35] *International Cooperation Between CERTS: WS38 Technical Diplomacy for Cybersecurity*. Panel presentation: Feakin. 2017. IGF.

[36] *Cyber Resilience. Playbook for Public-Private Cooperation*. 2018. WEF.

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

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