DiPLO
www.diplomacy.edu

Roles and Responsibilities of Communities and Users

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 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.

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 Communities and Users 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 communities and users by the remaining two actor clusters – states and the private sector – 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 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.[1]

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.[2]
- Engagement of communities and users in public-private partnerships aimed at policy development.[3]
- Policy development through provision of policy input and expertise.[4]

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.[5]
- Capacity building of civil society actors, through education.[6]
- 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.[7]
- Norms development whereby the technical community focuses on establishing technical standards, while civil society organisations mainly advocate for developing confidence-building

[1] *Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience*. 2012. WEF.

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

[3] *Understanding Demand for Cyber Policy Resources*. 2017. RTI Report for Hewlett Foundation.

[4] *Ibid*.

[5] *Global Agenda Council on Cybersecurity*. 2016. WEF.

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

[7] *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.

measures, as well as pressure for 'security by design' principles exerted through procurement decisions of actors within this cluster.[8]

- Ensure security, primarily their own, through abiding by internationally accepted best practices and standards and utilizing privacy and security technologies.[9] End-users are seen as bearing the responsibility of practicing good cyber hygiene and managing software patches.[10] 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.[11] 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.[12]
- Policy development through provision of policy input and independent advice.[13] 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.[14]
- 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.[15]

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.[16]

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:

[8] *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.

[9] *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.

[10] *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*. 2016. GCIG.

[11] *Stateless Attribution. Toward international accountability in cyberspace*. 2017. RAND.

[12] *A Role for Civil Society?* 2014. ICT4Peace.

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

[14] A Role for Civil Society? 2014. ICT4Peace.

[15] *Call to Protect the Public Core of the Internet*. 2017. GCSC.

[16] *A Role for Civil Society?* 2014. ICT4Peace.

- Ensuring security, their own[17], as well as that of end-users of installing technical safeguards for the ICTs they use.[18] Cooperation among ethical hackers and the wider ICT community is also seen as an important model contributing to security.[19]
- Policy development through provision of policy input advocating for a comprehensive approach encompassing all actors in the stakeholder community.[20]
- Responsible behaviour, mainly in terms of having all end-users meeting minimum cyber hygiene requirements.[21]

A recognition of the actor cluster already engaging in ensuring security through multi-stakeholder cooperation has already been made.[22]

Further questions for consideration

Should academia assume a greater role in cybersecurity policy development?

Academia in general has been seen as moving slower than other types of organisations, and less directly concerned with influencing policy, both by design and in effect. Despite conducting research, this sub-cluster of communities and users is seen as reluctant to take specific policy positions when probed for input or feedback. Should academia remain policy-neutral, providing solely the bare fact and figures, or should it engage in assuming a more policy-developing role, providing clear stances on different policy options on cybersecurity?[23]

To what extent can civil society effectively participate in the cybersecurity policymaking process?

Concerns have been raised that with the lack of specificity of the term “cybersecurity” in conjunction with the emergence of sovereignty considerations in cybersecurity policymaking may lead to re-couch all cybersecurity issues into the language of “national security” and warfare, preventing balanced policy making and fostering the adoption of drastic solutions such as network monitoring instead of other practical solutions more respectful of citizens’ rights. How realistic are concerns that an increasingly blurred line between sovereignty and cybersecurity could reduce civil society’s participation in the policymaking process and result in the involvement and lobbying of the security industry and law enforcement, opaque policy processes, strong military and intelligence interests, public-private partnerships modelled on traditional intelligence communities rather than Internet governance ones, and finally state-to-state interactions taking place in closed settings?[24]

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

[17] *Chair’s Statement*. 2015. Global Conference on Cyberspace.
[18] *The role and responsibilities of an effective regulator*. 2009. ITU.
[19] *Chair’s Statement*. 2015. Global Conference on Cyberspace.
[20] *The role and responsibilities of an effective regulator*. 2009. ITU.
[21] *Digital security risk management for Economic and Social Prosperity*. 2015. OECD. *Commonwealth Cybergovernance Model*. 2014. Commonwealth Telecommunications Organisation.
[22] *Chair’s Statement*. 2015. Global Conference on Cyberspace.
[23] *Understanding Demand for Cyber Policy Resources*. 2017. RTI report for the Hewlett Foundation’s Cyber Initiative.
[24] *Cybersecurity policy making at a turning point*. 2012. OECD.

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.[25]

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 cross-border technical communication and cooperation, or should they be politicised and used as part of the 'diplomatic toolkit' of states?[26]

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

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