Roles and Responsibilities of States

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, 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 different actors should take. When it comes to 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.

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 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 – the private sector 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 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 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

[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.

[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.

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]
- 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,

---

[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.

[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.

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]
- 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]

---

[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.

[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.

- 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]

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]

---

[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.

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

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]

---

[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. *International Cyber Norms*. 2016. Osula & Roigas (eds.). NATO CCD CoE. Hill, R. 2018. *Best practices in cyber security from intergovernmental*

- 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

---

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.

accounts or private data, using ICTs to steal intellectual 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]

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?[45]

How big of a role should the private sector have in providing cyber defence?

With resilience seen as the responsibility of private actors almost equally as that of the state – given ownership of critical infrastructure and numbers and type of potentially affected end-users – the private sector is increasingly expected to provide for active cyber defence. However, considerations of delegating a greater role in defence to the private sector, have also raised questions of potentially significant collateral consequences, for example, private sector hack-backs of an alleged public sector adversary.[46]

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?[47]

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

---

[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] *Ibid.*
[46] *Ibid.*
[47] *Ibid.*

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?[48]

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.[49]

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?[50]

Can/Should the principle of due diligence be applied to cyber activities?

The Tallinn Manual restated the law as follows:

States are required under international law to take appropriate steps to protect those rights. This obligation applies not only to criminal acts harmful to other States, but also, for example, to activities that inflict serious damage, or have the potential to inflict such damage, on persons and objects protected by the territorial sovereignty of the target State.

It is incontrovertible that states enjoy sovereignty over cyber infrastructure and activities located on their territory. But whether transit states—states through which the operations merely travel—bear a due diligence obligation is less clear.[51]

---

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

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

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

[51] Schmitt. M. 2015. *In Defense of Due Diligence in Cyberspace*. The Yale Law Journal Forum.