RESEARCH IN FOCUS

International Cybersecurity Norm Development: The Roles of States Post-2017

Jacqueline Eggenschwiler
University of Oxford
April 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

Once considered the primary purview of sovereign entities, processes of international norm-formation have experienced far-reaching phases of pluralisation. Non-state actors have come to inhabit central areas of global policymaking, which in turn has given rise to questions about the normative and legislative capabilities of governmental protagonists. In the context of cybersecurity, for example, political quarrels among state actors concerning the enactment of norms for responsible behaviour in the digital realm have created a flourishing environment for non-state actor initiatives. As a rising amount of normative pro-posals appears to emanate not from traditional, sovereign entities but from a collection of non-state actors, including private sector, civil society and multi-stakeholder organisations, a reassessment of the roles of sovereign actors is important for making sense of contemporary cybersecurity governance and understanding future policy trajectories. This paper finds that despite a strong increase in the number of non-state initiatives, governmental protagonists remain critical agents of cybersecurity norm-making. Effective provision of cybersecurity at a global level requires states to live up to their traditional roles as standard-setters and enforcers of norms. Given the complex and highly interconnected nature of cyberspace, they also have to assume additional roles, e.g. as sparring partners of non-state initiatives and meta-level orchestrators of normative responsibilities.

Key points

- International norm-formation has long been considered the exclusive purview of governmental actors. In the context of cybersecurity, this paradigm has come under increasing attack as a diverse group of non-state actors has come to actively contribute to the development of global rules for the digital realm.
- State-driven debates concerning the implementation of norms for responsible behaviour in cyberspace have yielded mixed results. However, with regard to stipulating red lines, governments continue to benefit from a unique combination of material and symbolic power sources.
- In order to move debates forward and make headway, states need to acknowledge the contributions of non-state actors and draw on their expertise and input for implementing security-enhancing norms and policies.
- Building confidence and creating stability in the use of Information and Communications Technologies (ICTs) requires public actors to live up to their traditional roles as standard-setters and enforcers of norms and take on additional roles, e.g. as sparring partners of non-state initiatives or meta-level orchestrators of normative responsibilities.

1. Introduction

As cybersecurity incidents are occurring ever more frequently, debates about international norms which regulate nefarious cyber activities capable of jeopardising economic, social and human systems have gained traction over the past few years.[1] Norms denote "sets of intersubjective understandings and collective expectations regarding the proper behaviour of states and other actors in a given context or identity".[2] They can be binding or non-binding and be of regulating, constituting or enabling character.

> **"[…] political quarrels among state actors concerning the enactment of norms for responsible behaviour in the digital realm have created a flourishing environment for non-state initiatives.**

Traditionally considered the primary purview of sovereign entities, processes of global norm-construction have seen far-reaching phases of pluralisation. Non-state actors have come to inhabit central areas of global policymaking, which in turn has given rise to questions about the normative and legislative capabilities of governmental protagonists. In the context of cybersecurity, political quarrels among state actors concerning the enactment of norms for responsible behaviour in the digital realm have created a flourishing environment for non-state initiatives. Various civil society organisations as well as large international corporations, such as Microsoft, Siemens and Telefónica, have issued non-binding frameworks directed at enhancing the stability and security of the virtual domain.[3]

As a rising amount of normative proposals appears to emanate not from traditional, sovereign entities but from a collection of non-state actors, including private sector, civil society and multi-stakeholder organisations, a reappraisal of the roles of sovereign actors is critical for making sense of contemporary cybersecurity governance and understanding future policy trajectories. Refuting claims of sovereign power erosion, this paper maintains that governmental protagonists remain critical agents of cybersecurity norm development.[4] Effective provision of cybersecurity at a global level requires states to live up to their traditional roles as standard-setters and enforcers of norms. This paper further holds that states have to take on additional roles, e.g. as sparring partners of non-state initiatives or meta-level orchestrators of normative responsibilities.[5]

---

[1] Tim Maurer, 'Cyber Norm Emergence at the United Nations', Belfer Center Discussoin Paper 2011-11, 2011, http://belfercenter.hks.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf; Martha Finnemore, 'Cybersecurity and the Concept of Norms', Carnegie Endowment for International Peace, 2017; Greg Austin, Bruce McConnell, and Jan Neutze, 'Promoting International Cyber Norms: A New Advocacy Forum', 2015, https://cybersummit.info/sites/cybersummit.info/files/BGCyberNorms_FINAL.pdf; Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', Contemporary Security Policy 33, no. 1 (13 April 2012): 148–70,; Roger Hurwitz, 'The Play of States: Norms and Security in Cyberspace', American Foreign Policy Interests 36, no. 5 (3 September 2014): 322–31.

[2] Annika Björkdahl, 'Norms in International Relations: Some Conceptual and Methodological Reflections', Cambridge Review of International Affairs 15, no. 1 (28 April 2002): 15,

[3] Smith, "A Digital Geneva Convention to Protect Cyberspace"; Siemens, "Time for Action: Building a Consensus for Cybersecurity"; Tikk et al., Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary; Global Commission on the Stability of Cyberspace, "Call to Protect the Public Core of the Internet."

[4] Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel, Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, ed. Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel (Farnham: Ashgate Publishing Limited, 2013), https://books.google.ch/books?id=ZBWGG0eF7zgC.

[5] Alex Grigsby, 'The End of Cyber Norms', Survival 59, no. 6 (2 November 2017): 109–22,

2. A brief recap of state-driven norm development efforts

Initially construed as a space free from intervention and control, the rising tide of threats confronting critical ICT infrastructures has spurred a shift in the perception of cyberspace.[6] Cyberspace has evolved from a matter of low politics to a matter of high politics.[7] It has become an area of strategic concern, a domain of power execution and a zone of conflict.[8] In the absence of coherent international ordinances pertaining to cybersecurity, calls for addressing destabilising behaviour in the virtual realm have been answered with voluntary, non-binding norms. "Norms [...] have emerged along with confidence- and capacity-building measures as the principal policy tools of choice to meet the shared vision of an open, secure, accessible, and peaceful ICT environment".[9]

First discussions concerning the creation of rules to curb malicious behaviour in cyberspace can be traced back to the mid-1990s. In 1996, the Council of the European Union endorsed a proposal put forward by the French government for a *Charter for International Cooperation on the Internet*.[10] At the time, "the French Minister for Information Technology expressed hope that the initiative would lead eventually to an accord comparable to the international law of the sea".[11] The French proposition was followed by a Russian bid in the remit of the UN General Assembly, which sought to ban information weapons and their use by way of legally binding rules. Moscow's draft resolution emerged amid a perceived Western dominance of the ICT landscape and gave rise to more institutionalised international discussions.

In reaction to Russia's proposal of 1998, and as a result of concerns over the appropriateness of legally binding provisions, particularly on the part of Western states, the UN commissioned a Group of Governmental Experts to study existing and emerging threats emanating from the digital realm and possible normative measures to address them. Since 2004, five GGEs of different compositions have convened; together, they have issued a total of three consensus reports, of which the 2013 and 2015 reports remain the most consequential for discussions concerning norms.[12]

The second consensus document of 2013 stipulated that international law, and in particular the United Nations Charter, applies to cyberspace and should serve as a bedrock for a secure, peaceful and openly accessible ICT environment.[13] Building on the 2013 consensus report, the third document reiterated the importance of the applicability of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by sovereign actors. The 2015 report put forward 11 norms of appropriate state behaviour in cyberspace, such as that "states should not

---

[6] John P Barlow, 'A Declaration of the Independence of Cyberspace', 1996; Neil Loughlin, 'The Benefits and Disadvantages of Post-Positivism in International Theory', E-International Relations, 2012, http://www.e-ir.info/2012/01/20/what-are-the-benefits-and-disadvantages-of-post-positivism-for- international-theory/; David R. Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace', Stanford Law Review 48, no. 5 (May 1996): 1367.

[7] Nazli Choucri and David D. Clark, 'Integrating Cyberspace and International Relations: The Co-Evolution Dilemma', SSRN Electronic Journal, no. 29 (2012): 1–14.

[8] Joseph S. Jr. Nye, 'The Regime Complex for Managing Global Cyber Activities', Global Commission on Internet Governance, Paper Series (Centre for International Governance Innovation and the Royal Institute for International Affairs, 2014).

[9] Kavanagh, "The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the the 21st Century," 10.

[10] Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers', Leiden Journal of International Law 30, no. 4 (2017): 877–99.

[11] Timothy S. Wu, 'Cyberspace Sovereignty? The Internet and the International System', Harvard Journal of Law & Technology 10, no. 3 (1998): 660.

[12] Ann Väljataga, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly', NATO CCDCOE, 2017, https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

[13] United Nations, General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/68/98 (24 June 2013).

knowingly allow their territory to be used for internationally wrongful acts using ICTs"; or "conduct or knowingly support ICT activity that intentionally damages critical infrastructure".[14]

The 2017 edition of the UNGGE was intended to continue the works of the preceding UNGGEs and was meant to further specify the provisions contained in the 2015 consensus document.[15] However, as a result of stark political and ideological differences, it failed to reach substantive agreement on issues including the applicability of international law to the use of ICTs by states and was eventually disbanded.[16]

Among observers of international cybersecurity norm-construction processes, the non-consensus outcome of the 2017 meeting sparked heated discussions and even led some commentators to proclaim the end of cybernorms and sovereign standard-setting.[17] While such declarations may carry some publicity-increasing value, they are misleading and short-sighted. For one thing, international norm-construction efforts rarely happen in hermetically sealed environments and do not simply end when governmental entities fail to reach consensus. Furthermore – and more importantly – vigorous debate and compromise allow for re-examination and meaningful reflection.

3. The rise of non-state actor initiatives: Mapping the stakeholders

Following the non-consensus outcome of the 2017 UNGGE as well as major cybersecurity incidents of transnational magnitude, such as WannaCry and Petya/NotPetya, non-state initiatives directed at fostering responsible behaviour in the digital domain have increased markedly.[18]

Scholarly literature has systematised and subsumed ideational efforts conducted by non-state actors under the umbrella of "*norm-entrepreneurship*".[19] Seeking to change prevailing patterns of behaviour, actors engaging in norm-entrepreneurship typically set out by suggesting normative ideas and then mobilising like-minded stakeholders or networks within and across states to endorse them.[20] "These alliances bring pressure to bear from above (transnationally) and below (domestically)", and help the standards proposed get more widely accepted.[21] The initiatives described below clearly exhibit elements

[14] United Nations, General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", para. 13(c), UN Doc. A/70/174 (22 July 2015).
[15] Endeavours to construct norms and build confidence among sovereign actors in response to ICT-related insecurities have also occurred outside the confines of the United Nations, e.g. in environments such as the African Union, the ASEAN Regional Forum (ARF), the Brazil, Russian Federation, India, China and South Africa (BRICS) grouping, the Council of Europe, the European Union, the Group of Seven (G7), the Group of 20 (G20), the Organization of American States (OAS), the Organization for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE) and the Shanghai Cooperation Organization (SCO). However, due to their limited substantive scope and geographic concentration, these fora have received considerably less attention than the UNGGEs.
[16] While Western proponents are mostly concerned with infrastructure protection in the sense of maintaining the confidentiality, integrity and availability of systems and networks, non-Western actors underscore state control over ICTs and the dissemination of information potentially harmful to their cultural and socio-political systems.
[17] Grigsby, 'The End of Cyber Norms'; Mačák, 'From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers'; Väljataga, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly'.
[18] Alex Hern, 'WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017', The Guardian, 2017, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
[19] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', International Organization 52, no. 4 (1998): 887–917.; Thomas Risse-Kappen, Stephen C. Ropp, and Kathryn Sikkink, The Power of Human Rights: International Norms and Domestic Change, Cambridge Studies in International Relations (Cambridge: Cambridge University Press, 1999).
[20] Wayne Sandholtz, International Norm Change, Oxford Research Encyclopedia of Politics (Oxford: Oxford University Press, 2017), 2.
[21] Ibid, 2.

of norm-entrepreneurship, yet extend beyond the traditional confines of awareness-raising commonly associated with the latter.

3.1. ICT4Peace

ICT4Peace has been involved in discussions concerning responsible behaviour in cyberspace since at least 2011. In 2011, ICT4Peace publicly called for a Code of Conduct for Cyberconflicts. The corresponding report entitled *Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyberspace* maintained that "nations […] need to examine and assess the need for modifying existing laws to address cyber-specific issues. At both […] national and international levels, taskforces [*sic*] need to be established including all the key players to exchange information, provide early warning and explore possible solutions to existing or future challenges".[22] More recently, in a joint initiative with Leiden University's Program for Cyber Norms, ICT4Peace has co-sponsored the publication of a Global Commentary on Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology, which brings together comments and guidance for understanding and operationalising the recommendations contained in the UNGGE reports of 2010, 2013 and 2015.

3.2. Microsoft

Microsoft was among the first corporate stakeholders to instigate debates about responsible conduct in cyberspace. In February 2017, Microsoft President and Chief Legal Officer Brad Smith introduced the idea of a Digital Geneva Convention to Protect Cyberspace. Grounded in the belief that deep-rooted collaboration between states, the private sector and civil society is needed to curb nefarious acts in the digital realm, the convention, as outlined by Smith, asks governments to "come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules, and get to work implementing them".[23] This move represented a rupture with Microsoft's earlier efforts to influence the policy debate about norms through research. The timing of this specific initiative, however – immediately after the WannaCry/Not-Petya attacks – has raised questions about the company's real intentions.

Faced with fairly cold reception by governmental protagonists, Microsoft's call for a Digital Geneva Convention to Protect Cyberspace was succeeded by the unveiling of a Cybersecurity Tech Accord 14 months later. With a view to defending and advancing the benefits of networked technologies for society, the Cybersecurity Tech Accord calls on private actors to observe four specific principles and behaviours. So far, the Cybersecurity Tech Accord has been acceded to by more than 70 enterprises, including leading S&P 500 companies such as Facebook, Inc., Symantec Corp. and Cisco Systems. In September 2018, Microsoft unveiled its latest initiative, the Digital Peace Now campaign. Announced during the seventh Global Citizen Festival, it calls on citizens to protect cyberspace, e.g. through measures of cyber-hygiene, and urges governments to refrain from endangering the global digital environment. To date, the petition has attracted more than 100, 000 signatories.[24]

3.3. Siemens

Two months before the launch of Microsoft's Cybersecurity Tech Accord, Siemens, alongside eight partner corporations, presented a Charter of Trust for a Secure Digital World. Adopted at the sidelines

[22] Daniel Stauffacher, Ricardo Sibilia, and Barbara Weekes, "Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyberspace" (Geneva, 2011), https://www.files.ethz.ch/isn/167402/Cyberpeace-Paper-December-2011.pdf

[23] The call also asks global technology companies to behave as neutral actors and recommends setting up an independent non-governmental organisation capable of investigating and publicly attributing (nation-state) cyberattacks, see Brad Smith, 'The Need For a Digital Convention', Microsoft, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv.

[24] Microsoft, 'Digital Peace Now', 2018, https://digitalpeace.microsoft.com/#dp-share.

of the 2018 Munich Security Conference, the charter calls for binding rules and postulates 10 principles, ranging from supply chain security to critical infrastructure certification. The charter recognises that "in order to keep pace with continuous advances in the market as well as threats from the criminal world, companies and governments must join forces and take decisive action. This means making every effort to protect the data and assets of individuals and businesses; prevent damage from people, businesses, and infrastructures; and build a reliable basis for trust in a connected and digital world".[25]

3.4. Global Commission on the Stability of Cyberspace

A year prior to the postulation of Siemens' Charter of Trust for a Secure Digital World, the 2017 Munich Security Conference saw the inauguration of the Global Commission on the Stability of Cyberspace (GCSC), an expert consortium composed of regionally diverse scholars, CEOs and current and former policymakers.[26] Having convened multiple times along major internet policy meetings, such as the Munich Security Conference, CyCon, Black Hat, the Global Conference on Cyber Space and GLOBSEC, the GCSC has put forward a total of eight norms geared towards fostering more responsible conduct in cyberspace.

Besides acting as providers of products and services or capacity builders, the aforementioned protagonists have also come to behave as diplomatic agents. Their proposals are explicitly targeted at the global level and consciously employ political language. Microsoft's allusion to the Geneva Conventions of 1949 or Siemens' reference to political constructs like a "Charter" are deliberate rhetorical devices that expose underlying political aspirations. In terms of agency and structure, the norm-building activities conducted by non-state actors hint at a shift in global regulation from state-centric forms of steering toward new, non-territorial, multi-actor modes of governance.[27]

Table 1. Overview of norms and proposed principles

Global Commission on the Stability of Cyberspace	> Norm to protect the public core of the internet > Norm to protect the integrity of electoral infrastructures > Norm to avoid tampering > Norm against commandeering ICT devices as botnets > Norm for states to create a vulnerability equities process > Norm to reduce and mitigate significant vulnerabilities > Norm on basic cyber hygiene as foundational defense > Norm against offensive cyber operations by non-state actors
ICT4Peace	> Adopt cybercrime legislation > Modify existing laws (where necessary) > Engage in cross-sectoral collaboration
Digital Peace Now	> Stop cyberwarfare

[25] Siemens, 'Charter of Trust: For a Secure Digital World', 2018, https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

[26] The Commission's expressed goal is the development of "proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace". Composed of 26 commissioners and supported by a research team and a governmental advisory network, the GCSC draws on a rich pool of technical and political expertise. According to one of its commissioners, Dr. Wolfgang Kleinwächter, "the GCSC has the potential to become a trusted source of inspiration for global internet policy making in the 2020s", see Wolfgang Kleinwächter, 'The Kaljurand Commission: Building Bridges Over Troubled Cyber-Water', 2017, http://www.circleid.com/posts/20171202_kaljarund_commission_building_bridges_over_troubled_cyber_water/.

[27] Andreas Georg Scherer, Guido Palazzo, and Dorothée Baumann, 'Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance', Business Ethics Quarterly 16, no. 04 (23 October 2006): 506.

Cybersecurity Tech Accord	> Protect all users and customers from nefarious cyber activities, regardless of geographical location > Oppose cyberattacks on civilian and corporate infrastructures > Empower and support users, customers and developers in their efforts to strengthen cybersecurity > Partner with like-minded entities, civil society and security researchers across proprietary and open source technologies to enhance cybersecurity
Digital Geneva Convention	> Refrain from attacking systems whose destruction would adversely impact the safety and security of private citizens > Refrain from attacking systems whose destruction could damage the global economy > Refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes > Refrain from using information and communications technology to steal the intellectual property of private companies > Refrain from inserting or requiring backdoors in mass-market commercial technology products > Agree to a clear policy for acquiring, retaining, securing, using and reporting of vulnerabilities > Exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise and not reusable > Agree to limit proliferation of cyber weapons > Limit engagement in cyber offensive operations > Assist private-sector efforts to detect, contain, respond and recover in the face of cyberattacks
Charter of Trust	> Ownership of cyber and IT security > Responsibility throughout the digital supply chain > Security by default > User-centricity > Innovation and co-creation > Education > Certification for critical infrastructure and solutions > Transparency and response > Regulatory framework > Joint initiatives

4. The roles of states in international cybersecurty norm development post-2017

While international deliberations concerning norms of appropriate behaviour in cyberspace have proven daunting and difficult, history has shown that concurrence and progress are possible even in the most

politicised and intricate cases – just look at the global nuclear non-proliferation regime or the Paris Climate Accord.[28]

Even though intergovernmental debates remain highly polarised and do not leave much room for optimism, neither the recent ideological split of the expert-led process nor the 2017 non-consensus outcome should be read as a dead-end of state-led norm development processes.[29] On the contrary, continued engagement on the parts of states is crucial for bringing normative efforts to fruition and maturity in the long term.[30]

With regard to stipulating norms of responsible behaviour in cyberspace, governmental protagonists continue to benefit from a unique combination of material (access to resources and position in the global economy) and symbolic (legitimacy/ability to invoke moral claims) power sources.[31] As default security providers, states remain key agents for assigning the "right" – i.e. democratically legitimised – meaning and weight to facts, determining issues of causality and defining appropriate remedies.[32]

> **"[…] it is particularly important for states to encourage complementary normative approaches in which both public and private actors have some capacity to contribute and employ their relevant comparative advantages.**

For quite some time, states have hidden behind a smokescreen of strategic ambiguity and have effectively neglected their customary functions as enforcers of normative commitments. Strategic ambiguity has let governmental protagonists engage in malicious cyber activities, such as espionage, sabotage or surveillance, with impunity. However, from both a tactical perspective and a political standpoint, strategic ambiguity is risky and misleading as it does not reduce the odds for fallout.[33] According to former State Department Cybersecurity Coordinator Christopher Painter, there is still no sense of consequence for violating norms of appropriate behaviour in cyberspace, which casts doubts on normative guarantees and significantly increases the probability for misinterpretation and escalation.[34]

Where substantive international discussions pertaining to standards of appropriate behaviour in cyberspace appear inoperable, consistent state practice – even by a small number of committed public actors – can offer means for further progress. Stringent state behaviour centred on the observance and enforcement of proposed norms can act as a proxy for more formalised measures and introduce much-needed red lines.[35] For those red lines to have a restraining effect, however, there needs to be a credible belief in their effectuation and follow-through (either directly or indirectly).

---

[28] John Gerard Ruggie, 'The Social Construction of the UN Guiding Principles on Business and Human Rights', 2017, https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/workingpaper_67_0.pdf; Ann P. Kinzig et al., 'Social Norms and Global Environmental Challenges: The Complex Interaction of Behaviors, Values, and Policy', BioScience 63, no. 3 (March 2013): 164–75.

[29] "The international community is now faced with two parallel and competing processes, ostensibly dealing with the same subject matter, which will challenge both the capacities and the coherence of the UN going forward", see Paul Meyer, 'Visions on the Future of Cyberspace Clash at the UN', ICT4Peace, 2018, https://ict4peace.org/activities/visions-on-the-future-of-cyberspace-clash-at-the-un/.

[30] Meyer.

[31] From an international legal perspective, states are the only entities able to claim some form of democratic legitimacy for proposing standards of responsible behaviour in cyberspace and holding other actors to account. From a material standpoint, states have at their disposal the necessary resources and political capabilities to engage in long-term norm development processes.

[32] Eneken Tikk and Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy', 2017, http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf.

[33] Mariarosaria Taddeo, 'Deterrence by Norms to Stop Interstate Cyber Attacks', Minds and Machines 27, no. 3 (2017): 387–92,

[34] Charlie Mitchell, 'Still No Sense of Consequence for Violating Cyber Norms of Behavior', Black Hat Conference, 2018, https://insidecybersecurity.com/daily-news/panel-still-no-sense-consequence-violating-cyber-'norms'-behavior.

[35] Tikk and Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy"; Kavanagh, "The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the the 21st Century."

In addition to their traditional responsibilities as norm setters and enforcers, governmental protagonists have to assume new roles. In light of increasing non-state actor engagement in processes of international cybersecurity norm development, there is scope for further extension of sovereign functions.

While the 2013 and 2015 UNGGE reports did not specify rules of engagement between state and non-state actors, they did acknowledge that there is merit in establishing and, where applicable, expanding linkages among these entities. It was noted, for example, that while sovereign protagonists bear primary responsibility for national security and the safety of their citizens, including in the digital realm, international cooperation and cross-sectoral assistance are of vital importance for states to secure ICTs and warrant their peaceful use. Exchanges among governmental and non-governmental Computer Emergency Response Teams (CERTs) were mentioned as one example for fruitful policy exchange and political dialogue.

5. Dealing with non-state actors

Given that as much as 90 percent of critical network infrastructures are owned and operated by private entities, and that non-state actors are actively injecting their views and proposals into international cybersecurity norm development processes, states have to start engaging as sparring partners of non-state initiatives and meta-level orchestrators of normative responsibilities.[36] The latter suggests a pooling or sharing of traditional responsibilities with private actors vis-à-vis the development and effectuation of standards for appropriate behaviour in cyberspace, while the former involves an extension of public support for non-state efforts.

> “
>
> **[…] to overcome normatively-grounded ideological divides, it is important for Western state and non-state actors to appeal to non-Western stakeholders, actively engage with their ideational concepts and identify areas of strategic overlap.**

The Paris Call for Trust and Security in Cyberspace, also known as the Paris Call, adopted in November 2018, may prove to offer an important trajectory in this regard.[37] Unveiled at the 12th Internet Governance Forum (IGF) in Paris, the Paris Call aims to develop common principles for securing cyberspace through collaborative efforts across existing international platforms and mechanisms.[38] Open for endorsement by state and non-state actors alike, the Paris Call represents a high-level, non-binding political declaration.

Cognisant of the distributed nature of cyberspace and the need for more meaningful collaboration, the Paris Call advances nine objectives that respond to concerns of both public and private entities. These include the prevention of ICT-enabled theft of proprietary information and intellectual property as well as the coordinated disclosure of ICT vulnerabilities.[39]

Rather than reinventing the wheel in terms of normative prescriptions, the Paris Call constitutes an attempt at realigning fragmented discussions of norms that have been scattered across multiple fora. While France’s proposal has seen fairly broad uptake among governments, private industry, the technical community, researchers, non-governmental organisations and civil society, there are a number of notable public abstentions, including the United States, Russia, China, Iran and Israel.[40]

---

[36] Ibid, 29.
[37] Ministère de l’Europe et des Affaires Étrangères, ‘Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace’, French Foreign Policy, 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.
[38] Ibid.
[39] Ibid.
[40] Louise Matsakis, ‘The US Sits Out an International Cybersecurity Agreement’, WIRED, accessed 13 December 2018, https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

Post-2017, and considering the proliferation of non-state actor activities, the bundling of different initiatives as well as the orchestration of relevant responsibilities will be key roles for public sector protagonists going forward. In this context, it is particularly important for states to encourage complementary normative approaches in which both public and private actors have some capacity to contribute and employ their relevant comparative advantages. Greater alignment and focus on complementarity can further help to improve initiatives and strengthen normative commitments. In addition, in order to overcome normatively-grounded ideological divides, it is important for Western state and non-state actors to appeal to non-Western stakeholders, actively engage with their ideational concepts and identify areas of strategic overlap.[41]

6. Conclusion

Given the distributed nature of the digital realm, arguments in favour of unilateral norm-enactment by states are unsustainable. Non-state actors actively participate in normative debates. Indeed, the diplomatic engagement of non-state actors points to a need for more collaborative forms of governance in which business enterprises, civil society organisations and expert communities participate in joint steering efforts with sovereign authorities.

Governments are asked to more genuinely acknowledge non-state actors' technological expertise, ownership and resource structures, as well as their international standing, which give them the capacity to meaningfully contribute to the implementation of measures intended to increase international stability and security in the use of ICTs. Non-state actors can directly support state actors in fulfilling their normative commitments by refraining from backing sovereign entities in acts of subversion and offensive assault, providing assistance on questions of attribution and ensuring resilience of critical infrastructures. Identifying areas of normative complementarity is key for moving discussions forward and achieving implementation of norm-based red lines.

While from a scholarly and policy perspective, closer normative exchanges between state and non-state actors will raise intricate questions concerning transparency (How are checks and balances ensured?) and legitimacy (How can the execution of normative authority of non-elected entities be justified?), "it is time to go beyond sharing and ad hoc cooperation, to collaboration at scale across borders, stakeholders, and sectors".[42] In order to move from cyber insecurity to cyber stability, it is critical that public systems interact with private systems in a symbiotic way.[43] The enactment of peace and security in the virtual realm requires setups with greater legislative, administrative and adjudicatory flexibility, consisting of both public and private entities operating in their complementary roles.[44]

[41] Companies like Kaspersky aim to contribute to the normative discussion by launching their own initiatives. For instance, the Global Transparency Initiative in Zurich serves as a facility for trusted partners to access reviews of the company's code, software updates and threat detection rules, along with other activities. The company has also made statements against the militarisation of cyberspace and the 'world-war-web'. See for instance: https://www.kaspersky.com/about/policy-blog/general-cybersecurity/the-collateral-damage-of-the-world-war-web; https://www.kaspersky.com/about/policy-blog/general-cybersecurity/how-to-deal-with-militarizing-cyberspace.

[42] Jason Healey, 'Innovation on Cyber Collaboration: Leverage at Scale', vol. 1, 2018, 1, http://www.atlanticcouncil.org/images/publications/Innovation-Cyber-WEB.pdf.

[43] Larry Catá Backer, 'Private Actors and Public Governance Beyond the State: The Multinational Corporation, the Financial Stability Board, and the Global Governance Order', Indiana Journal of Global Legal Studies 18, no. 2 (2011): 101–55,

[44] Daniel Bodansky, Legitimacy, ed. Daniel Bodansky, Jutta Brunnée, and Ellen Hey, The Oxford Handbook of International Environmental Law (Oxford: Oxford University Press, 2008), 4.

About the author

Jacqueline Eggenschwiler is a doctoral researcher at the University of Oxford. Her research looks at the contributions of non-state actors to processes of global cybersecurity norm formation and corresponding governance implications. Jacqueline holds degrees in International Affairs and Governance, International Management, and Human Rights from the University of St. Gallen and the London School of Economics and Political Science.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.