Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector

Framework Document, November 2018

Authors:

Jaqueline Eggenschwiler

ETH zürich

About

Under the auspices of the Geneva Dialogue on Responsible Behaviour in Cyberspace, launched by the Swiss Federal Department of Foreign Affairs (FDFA) in 2018, this document provides background information on private sector initiatives concerned with developing rules of the road for cybersecurity. It maps existing normative efforts, offers conceptual anchor points for thinking about the roles and responsibilities of private sector actors in the context of international peace and security in the digital realm, and reports on the industry relevant outcomes of the Geneva Dialogue on Responsible Behaviour in Cyberspace held on 1-2 November 2018 in Geneva.

Contents

Introduction

Against the background of proliferating cybersecurity incidents, debates about the need for international norms regulating nefarious cyber activities capable of jeopardising economic, social and human systems have gained increasing 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.

For decades, the United Nations General Assembly (UN GA), and in particular its First Committee on Disarmament and International Security, has "served […] as the centre of gravity for diplomatic negotiations over information technologies and their perceived and real effects."[3] Spurred by Russian efforts to establish an international legal regime pertaining to information security, the UN GA's First Committee called into life a Group of Governmental Experts (UN GGE) to study existing and emerging threats emanating from the digital realm and possible normative measures to address them. The first of a total of five groups met in 2004. While the UN GGEs meeting between 2009-2015 managed to issue non-binding consensus reports, the groups convening between 2004-2005 and 2016-2017 did not produce corresponding documents.[4]

Subsequent to the 2016-2017 UN GGE's inability to agree on a consensus report, and following major cybersecurity incidents of transnational magnitude, including WannaCry and Petya/NotPetya, there has been a noticeable surge in the number of private sector initiatives directed at fostering responsible behaviour in the virtual domain.[5] Examples include, among others, Microsoft's proposal for a *Digital Geneva Convention* as well as its adoption of a *Cybersecurity Tech Accord*, Google's *New Legal Framework for the Cloud Era,* Siemens' conclusion of a *Charter of Trust*, as well as Telefónica's *Manifesto for a New Digital Deal*.

[1] Tim Maurer, 'Cyber Norm Emergence at the United Nations' (2011) <http://belfercenter.hks.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf> accessed 20 February 2018; Martha Finnemore, 'Cybersecurity and the Concept of Norms' (2017) <http://carnegieendowment.org/files/Finnemore_web_final.pdf>; 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' (2012) 33 Contemporary Security Policy 148 <https://www.tandfonline.com/doi/full/10.1080/13523260.2012.659597>; Roger Hurwitz, 'The Play of States: Norms and Security in Cyberspace' (2014) 36 American Foreign Policy Interests 322 <http://www.tandfonline.com/doi/abs/10.1080/10803920.2014.969180>.

[2] Annika Björkdahl, 'Norms in International Relations: Some Conceptual and Methodological Reflections' (2002) 15 Cambridge Review of International Affairs 9, 15 <http://www.tandfonline.com/doi/full/10.1080/09557570220126216>.

[3] Camino Kavanagh, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the the 21th Century' (2017) 15 <http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf>.

[4] 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> accessed 5 July 2018.

[5] 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> accessed 6 February 2018.

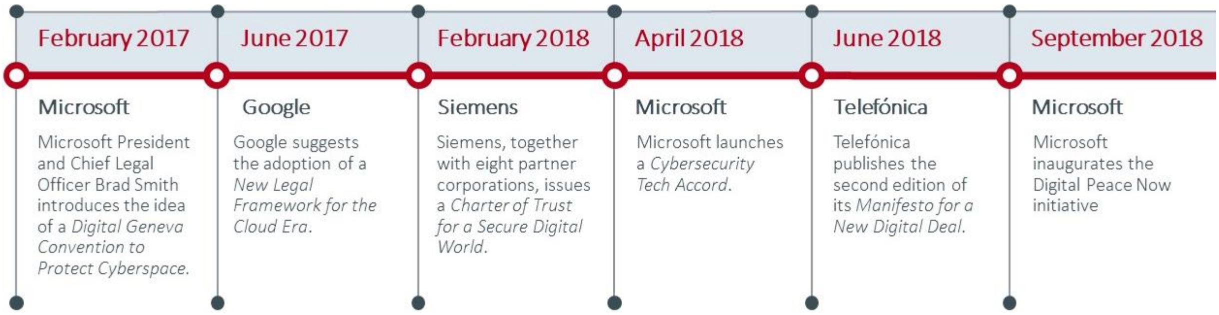

February 2017
Microsoft
Microsoft President and Chief Legal Officer Brad Smith introduces the idea of a Digital Geneva Convention to Protect Cyberspace.
June 2017
Google
Google suggests the adoption of a New Legal Framework for the Cloud Era.
February 2018
Siemens
Siemens, together with eight partner corporations, issues a Charter of Trust for a Secure Digital World.
April 2018
Microsoft
Microsoft launches a Cybersecurity Tech Accord.
June 2018
Telefónica
Telefónica publishes the second edition of its Manifesto for a New Digital Deal.
September 2018
Microsoft
Microsoft inaugurates the Digital Peace Now initiative

Figure 1: Timeline of leading private sector initiatives
Source: Author

In view of considerable political contestation at the intergovernmental level and a persisting need for security-enhancing cross-sectoral collaboration, this report examines the roles and responsibilities of private sector actors in contributing to international peace, security and stability vis-à-vis the malicious use of cyberspace.

This report is structured along four sections. The first section highlights extant private sector security practices and brings together key initiatives directed at advancing norms for responsible behaviour in cyberspace. The second section analyses these efforts and identifies corresponding private sector role profiles and responsibilities. The third section synthesises the norm-construction endeavours. The fourth section reports on the outcomes of the private sector expert panel as well as the private sector breakout session conducted on 1-2 November 2018 as part of the Geneva Dialogue on Responsible Behaviour in Cyberspace, and offers a short conclusion.

Extant Security Practices

Industry participation has been central to the growth and spread of ICT. As developers of products and suppliers of services such as end-point protection or technology consulting, corporate stakeholders have made important contributions to the "international […] architecture for the governance of cyber-space."[6] As owners of large parts of critical network infrastructures and technology platforms, they have come to wield considerable influence over key aspects of cyberspace and human existence. "Internet companies have become central platforms for discussion and debate, information access, commerce and human development. They collect and retain the personal data of billions of individuals, including information about their habits, whereabouts and activities, and often claim civic roles."[7]

Initially regarded as an issue of subsidiary importance (as something *nice to have*), cybersecurity has become front and centre on many board agendas, and has seen integration into enterprise risk management frameworks. Corporate committees have taken note of the perils emanating from digital technologies and have taken measures to address risks to critical infrastructures, business continuity, intellectual property, trade secrets and consumer privacy.

[6] Roxana Radu, 'Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace' in Jan-Frederik Kremer and Benedikt Müller (eds), *Cyberspace and International Relations* (Springer Berlin Heidelberg 2014) 4 <http://link.springer.com/10.1007/978-3-642-37481-4>.

[7] United Nations Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2018) para 9 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>.

While being active developers and implementers of security measures, private sector actors have at the same time also contributed to heightened levels of insecurity. By speeding up product development lifecycles, pushing out insecure products (for example in the context of IoT), and failing to update and maintain legacy systems, they have furthered the prevalence of systemic vulnerabilities.[8] Moreover, as part of their protective measures, some enterprises have engaged in offensive cyber operations, arguing that states are lacking the necessary capacity to adequately defend their interests and safeguard their existence. Such practices, however, including hack-backs, are unconducive to international cybersecurity and -stability. Not only do they have the potential to result in serious disruption and harm, but increase the chances for escalation and fallout.[9]

As the number and sophistication of cyberattacks continue to increase, private sector actors have recently also been seen to resort to more normative measures.

Mapping of Leading Normative Initiatives

In addition to operating as software developers, platforms of exchange and centres of expertise, business enterprises have come to act as proposers of international standards for responsible behaviour.

Microsoft's Digital Geneva Convention

Among the first private stakeholders to instigate debates about responsible conduct in cyberspace was Microsoft.[10] Following preceding efforts in 2013, 2014, and 2016, in February 2017, Microsoft President and Chief Legal Officer Brad Smith introduced the idea of a *Digital Geneva Convention to Protect Cyberspace*.[11] Grounded in the belief that deep-rooted collaboration among states, and between states, the private sector and civil society is needed to curb nefarious doings in the digital realm, the convention as outlined by Smith, asks governments to:

- "Refrain from attacking systems whose destruction would adversely impact the safety and security of private citizens (i.e., critical infrastructures, such as hospitals, electric companies).
- Refrain from attacking systems whose destruction could damage the global economy (e.g., integrity of financial transactions), or otherwise cause major global disruption (e.g., cloud-based services).

[8] Although the development of fully secure software of nontrivial size and complexity is illusionary, premature software releases to meet customer demand without adequate care for security introduce considerable dangers. See also Jane Chong, 'U.S. Cybersecurity: Why Is Software So Insecure?' (*The New Republic*, 2013) <https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure> accessed 12 September 2018.

[9] Hack-back refers to a type of active cyber defence conducted by a victim (on a perpetrator's infrastructure), in reaction to an initial attack, and with the intention of inflicting repercussive harm or gaining retribution.

[10] Microsoft Security Response Center, 'Announcing Coordinated Vulnerability Disclosure' (*TechNet*, 2010) <https://blogs.technet.microsoft.com/msrc/2010/07/22/announcing-coordinated-vulnerability-disclosure/> accessed 8 August 2018.

[11] Microsoft, 'Five Principles for Shaping Cybersecurity Norms' (2013) <https://www.microsoft.com/en-us/cybersecurity/content-hub/five-principles-for-shaping-cybersecurity-norms>; Angela McKay and others, 'International Cybersecurity Norms' (2014) <https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/>; Scott Charney and others, 'From Articulation to Implementation: Enabling Progress on Cybersecurity Norms' (2016) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8>; 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> accessed 9 July 2018.

- 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, including trade secrets or other confidential business information, to provide competitive advantage to other companies or commercial sectors.
- 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 – that reflects a strong mandate to report them to vendors – in mass market products and services.
- Exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable. States should also ensure that they maintain control of their weapons in a secure environment.
- Agree to limit proliferation of cyber weapons. Governments should not distribute, or permit others to distribute, cyber weapons and should use intelligence, law enforcement, and financial sanctions tools against those who do.
- Limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.
- Assist private sector efforts to detect, contain, respond, and recover in the face of cyberattacks. In particular, enable the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs). Intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals."[12]

Furthermore, it pleads global technology companies to behave as neutral actors, and recommends the setting-up of an independent non-governmental organisation capable of investigating and publicly attributing (nation-state) cyberattacks.[13]

Google's New Legal Framework for the Cloud Era

Similarly concerned with the stipulation of more up-to-date policies and norms, in June 2017, Google suggested the adoption of a *New Legal Framework for the Cloud Era*.[14] According to Senior Vice President and General Counsel, Kent Walker, rules and principles underpinning digital evidence-gathering are antiquated, and "due for a fundamental realignment in light of the rapid growth of technology that relies on the cloud, the very real security threats that face people and communities, and the expectations of privacy that internet users have in their communications."[15]

[12] Brad Smith, 'A Digital Geneva Convention to Protect Cyberspace' (2017) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>.

[13] Smith, 'The Need For a Digital Convention' (n 11); Tim Maurer and Kathryn Taylor, 'Outlook on International Cyber Norms: Three Avenues for Future Progress' (*Just Security*, 2018) <https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/> accessed 9 July 2018.

[14] Stephanie Condon, 'Google Pitches New Legal Framework for Cross-Border Data Handling' (*ZDNet*, 2017) <https://www.zdnet.com/article/google-pitches-new-legal-framework-for-cross-border-data-handling/> accessed 19 July 2018.

[15] Kent Walker, 'Digital Security and Due Process: A New Legal Framework for the Cloud Era' (*Google*, 2017) <https://www.blog.google/outreach-initiatives/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/> accessed 5 July 2018.

Google's suggested legal framework rests on two overarching principles. The first principle maintains that sovereign actors which have subscribed to baseline standards of privacy, human rights, and due process, "should be able to directly ask service providers for user data pertaining to serious crimes within their borders and users within their jurisdiction."[16] The second principle holds that countries which have endorsed these baseline standards should enter into bilateral agreements to speed up lengthy Mutual Legal Assistance Treaty (MLAT) processes and govern cross-border evidence-gathering more efficiently.[17]

While focused on digital evidence gathering, in more abstract terms, Google's effort speak to an underlying corporate demand for clear guidance and agreed upon frameworks concerning critical questions of cybersecurity.

Siemens' Charter of Trust for a Secure Digital World

Subsequent to Google's proposal of June 2017, Siemens, together with eight partner corporations, issued a *Charter of Trust for a Secure Digital World*.[18] Adopted at the side-lines of the 2018 Munich Security Conference, the charter calls for binding rules, and postulates ten principles ranging from ownership of cyber and IT security, responsibility throughout the digital supply chain, security by default, user-centricity, innovation and co-creation, to education, certification for critical infrastructure and solutions, transparency and response, regulatory framework, and joint initiatives.[19]

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."[20]

Microsoft's Cybersecurity Tech Accord

Microsoft's call for a *Digital Geneva Convention to Protect Cyberspace* was succeeded by the unveiling of a *Cybersecurity Tech Accord,* a year and two months later. With a view to defending and advancing the benefits of networked technologies for society, the *Cybersecurity Tech Accord* calls on private sector actors to observe four principles and behaviours, namely to:

[16] ibid.

[17] Condon (n 14); Kent Walker, 'Digital Security and Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era' (2017) <https://www.blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf>.

[18] 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> accessed 11 July 2018.

[19] Siemens, 'Time for Action: Building a Consensus for Cybersecurity' (*Cybersecurity*, 2018) <https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html> accessed 3 July 2018; Garrett Hinck, 'Private-Sector Initiatives for Cyber Norms: A Summary' (*Lawfare*, 2018) <https://www.lawfareblog.com/private-sector-initiatives-cyber-norms-summary> accessed 25 June 2018; Joe Kaeser, 'Working Together for More Security in the Digital World' (*LinkedIn Pulse* , 2018) <https://www.linkedin.com/pulse/working-together-more-security-digital-world-joe-kaeser> accessed 3 August 2018.

[20] Siemens (n 18) 1.

- 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 protection.
- Partner with like-minded entities, civil society, and security researchers, across proprietary and open source technologies, to enhance cybersecurity.[21]

So far, the *Cybersecurity Tech Accord* has been acceded to by more than 60 enterprises, including leading S&P 500 companies such as Facebook Inc., Symantec Corp., and Cisco Systems.[22] Others tech giants, including Google, Amazon and Apple have not yet joined the club of signatories.[23]

Telefónica's Manifesto for a New Digital Deal

Following Microsoft's conclusion of a *Cybersecurity Tech Accord*, on 25 June 2018, global telecommunications provider Telefónica published the second edition of its *Digital Manifesto*.[24] Building on the idea of a social contract, Telefónica holds that in order to keep reaping the benefits of digital technologies, it is necessary to modernise policies and norms to ensure fair competition and innovation. To that end, a *Digital Constitution*, a new *Digital Bill of Rights* to protect key human values and fundamental rights is required. Such a contract, so Telefónica, needs to be as human-centric as possible and rest on the involvement and support of as many stakeholders as possible.[25]

Revolving around five core principles, Telefónica's *Manifesto for a New Digital Deal* maintains that:

- Digitalisation should be an inclusive process, in which everyone is able to participate.
- Social and fiscal policies have to be adapted to the realities of current market conditions and digital companies.
- Users ought to have transparent knowledge of and control over their data and corresponding use thereof.
- Global providers of digital services should act responsibly and be committed to social development.
- Social policy and citizens' rights have to be modernised.[26]

[21] Brad Smith, '34 Companies Stand Up for Cybersecurity with a Tech Accord' (*Microsoft*, 2018) <https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/> accessed 10 July 2018.

[22] Cybersecurity Tech Accord, 'Cybersecurity Tech Accord' (2018) <https://cybertechaccord.org/accord/> accessed 10 July 2018.

[23] Hinck (n 19).

[24] The first edition of the Manifesto was launched in 2014. Telefónica, 'A Digital Manifesto: An Open and Safe Internet Experience For All' (2014) <https://www.telefonica.com/documents/341171/362460/20140410_A_Digital_Manifesto_ING_FINAL_reviewed.pdf/978031f0-d352-4f65-9c3c-b7d70fddf407>.

[25] Markus Haas, 'We Need a New Digital Deal So That Everyone Benefits From Digitalisation' (*Telefónica*, 2018) <https://www.telefonica.de/fixed/news/6135/article-by-ceo-markus-haas-we-need-a-new-digital-deal-so-that-everyone-benefits-from-digitalisation.html> accessed 11 July 2018.

[26] Telefónica, 'A Manifesto for a New Digital Deal' (2018) <https://www.telefonica.com/digital-manifesto/assets/a_manifiesto_for_a_new_digital_deal.pdf>.

Microsoft's Digital Peace Now Campaign

In addition to and in consonance with the Cybersecurity Tech Accord and the call for a Digital Geneva Convention, in September 2018, Microsoft unveiled its Digital Peace Now campaign. Announced during the seventh Global Citizen Festival, the Digital Peace Now initiative calls on citizens to protect cyberspace (e.g. through measures of cyber hygiene) and urge governments to refrain from endangering the global digital environment. To date, the petition has been supported by more than 100'000 signatories.[27]

Below table offers a short overview of the private sector initiatives introduced above.

Framework	Digital Geneva Convention	New Legal Framework for the Cloud Era	Charter of Trust for a Secure Digital World	Cybersecurity Tech Accord	Manifesto for a New Digital Deal	Digital Peace Now
Issuer	Microsoft	Google	Siemens	Microsoft	Telefónica	Microsoft
Number of signatories	N/A	N/A	16	69	N/A	>100'000
Principal addressees	State actors	State actors	Industry proponents	Industry proponents	State actors, industry proponents	Civil society

Figure 2: Overview of leading private sector initiatives
Source: Author

Analysis of Roles and Responsibilities

Although there is little overlap between the initiatives in terms of organisational membership and solicitation, all five frameworks have as their declared goals the instigation of rules for responsible behaviour in the virtual realm, albeit with different areas of focus.[28] And while the key drivers for corporate engagement on issues relating to international security and stability may be commercial in nature, at least to the extent that factors such as the reduction of costs and risks, the acquisition of competitive advantage, the development of corporate reputation and legitimacy, as well as the pursuit of win-win outcomes through synergistic value creation are taken into account, the proposals introduced above all display considerable degrees of normativity.[29]

[27] Microsoft, 'Digital Peace Now' (2018) <https://digitalpeace.microsoft.com/#dp-share> accessed 4 December 2018.

[28] While Microsoft and Siemens are mostly concerned with infrastructure-related aspects, Telefónica focuses on socio-economic questions, and Google zooms in on legal issues.

[29] Elizabeth C Kurucz, Barry A Colbert and David Wheeler, *The Business Case for Corporate Social Responsibility*, vol 1 (Andrew Crane and others eds, Oxford University Press 2009) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199211593.001.0001/oxfordhb-9780199211593-e-004>; Matteo Tonello, 'The Business Case for Corporate Social Responsibility'

Scholarly literature has systematised and subsumed ideational efforts conducted by private sector actors under the umbrella of *norm-entrepreneurship*.[30] Seeking to change prevailing patterns of behaviour, actors engaging in *norm-entrepreneurship* typically set out by suggesting normative ideas and mobilising like-minded stakeholders or networks, both within and across states, to endorse them.[31] "These alliances bring pressure to bear from above (transnationally) and below (domestically)," and help the standards proposed get more widely accepted.[32] To garner support, *norm-entrepreneurs* rely on a variety of different instruments, including incentives, persuasion, and socialisation.[33] "Norm entrepreneurs are critical for the emergence of normative standards because they call attention to issues or even create issues by using language that names, interprets, and dramatises them."[34]

The initiatives launched by Microsoft, Siemens, Telefónica, and Google clearly exhibit elements of *norm-entrepreneurship*, yet extend beyond the traditional confines of awareness raising, capacity building, and advocacy commonly associated with the latter. Besides acting as providers of products and services corporate stakeholders have come to behave as diplomatic protagonists. Their proposals are explicitly targeted at the international level and consciously employ political language. Microsoft's allusion to the Geneva Conventions of 1949 or Telefónica's and Siemens' reference to political constructs such as *Manifesto* and *Charter* are deliberate rhetorical devices, signposting underlying political aspirations. From an agency-oriented perspective, the norm-building activities conducted by private sector actors reflect a substantial extension of corporate authority. From a structural point of view, they suggest a shift in global regulation from state-centric forms of steering toward new non-territorial, multi-actor modes of governance.[35]

(*Harvard Law School Forum on Corporate Governance and Financial Regulation*, 2011) <https://corpgov.law.harvard.edu/2011/06/26/the-business-case-for-corporate-social-responsibility/#8b> accessed 18 July 2018.

[30] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change' (1998) 52 International Organization 887 <http://journals.cambridge.org/abstract_S0020818398440608>; Thomas Risse-Kappen, Stephen C Ropp and Kathryn Sikkink, *The Power of Human Rights: International Norms and Domestic Change* (Cambridge University Press 1999).

[31] Wayne Sandholtz, 'International Norm Change' (2017) 1 Oxford Research Encyclopedia of Politics 1, 2 <http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-588>.

[32] ibid.

[33] Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110 The American Journal of International Law 425, 445 <http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425>.

[34] Finnemore and Sikkink (n 30) 897.

[35] Andreas Georg Scherer, Guido Palazzo and Dorothée Baumann, 'Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance' (2006) 16 Business Ethics Quarterly 505, 506 <https://www.cambridge.org/core/product/identifier/S1052150X00011040/type/journal_article>.

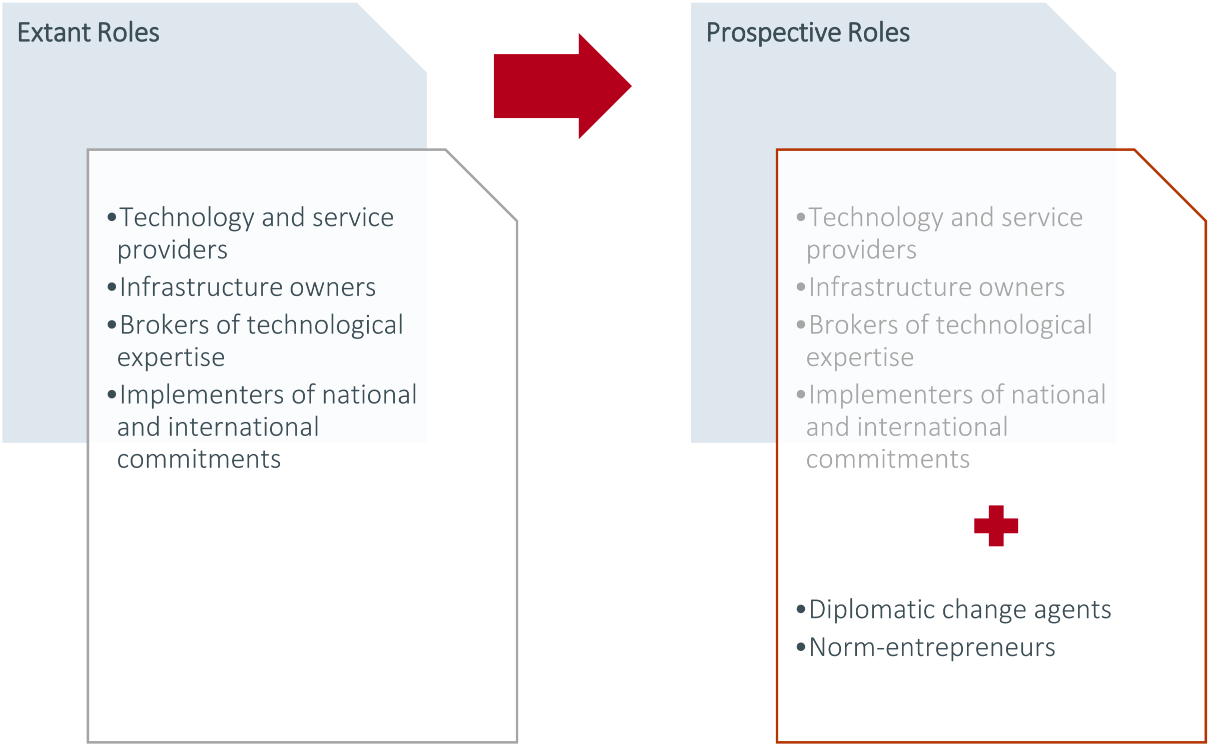
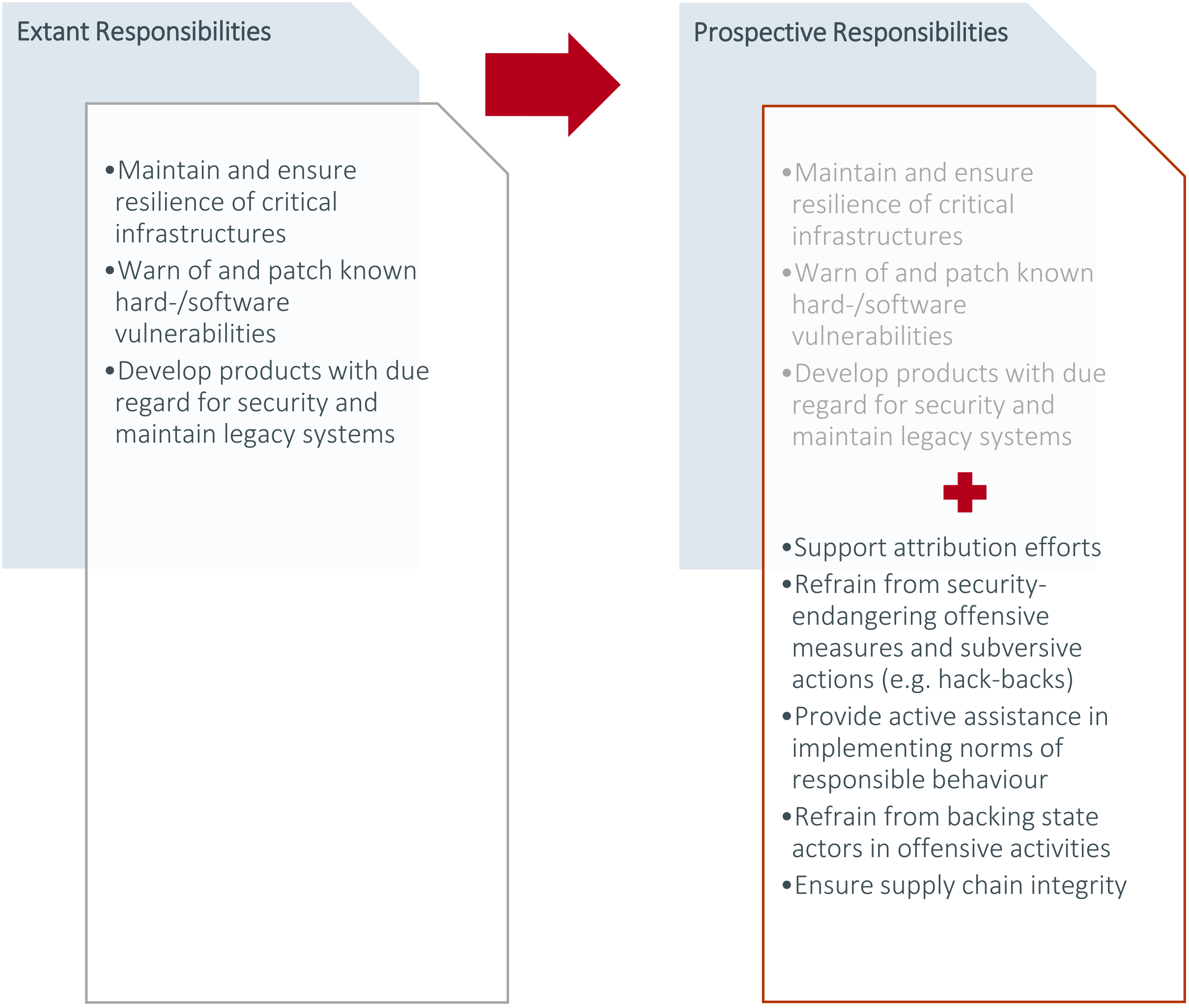

Extant Roles
•Technology and service providers
•Infrastructure owners
•Brokers of technological expertise
•Implementers of national and international commitments
Prospective Roles
•Technology and service providers
•Infrastructure owners
•Brokers of technological expertise
•Implementers of national and international commitments
•Diplomatic change agents
•Norm-entrepreneurs

Figure 3: Shift in Role Profiles of Private Actors
Source: Author

The initiatives introduced above respond in important ways to calls for corporate engagement included in the UN GGE reports of 2010, 2013, and 2015.[36] The latter make reference to the responsibilities of private sector actors namely with regard to participating or engaging in cooperative and confidence building measures, ICT security and capacity building assistance, Public Private Partnerships, exchanges of information between CERTs and within and beyond CERT communities. Paragraph 31 of the 2015 UN GGE report, for example, holds that "while states have a primary responsibility to maintain a secure and peaceful ICT environment, international cooperation would benefit from the appropriate participation of the private sector, academia and civil society."[37]

[36] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2010) <http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201>; United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2013) <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>; United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>.

[37] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (n 36) para 31.



Extant Responsibilities

- Maintain and ensure resilience of critical infrastructures
- Warn of and patch known hard-/software vulnerabilities
- Develop products with due regard for security and maintain legacy systems

Prospective Responsibilities

- Maintain and ensure resilience of critical infrastructures
- Warn of and patch known hard-/software vulnerabilities
- Develop products with due regard for security and maintain legacy systems

+

- Support attribution efforts
- Refrain from security-endangering offensive measures and subversive actions (e.g. hack-backs)
- Provide active assistance in implementing norms of responsible behaviour
- Refrain from backing state actors in offensive activities
- Ensure supply chain integrity

Figure 4: Shift in Responsibilities of Private Actors
Source: Author

Given that as much as 90% of critical network infrastructures are owned and operated by private sector companies, and that non-state actors are actively injecting their views and proposals into international cybersecurity norm development processes, private sector actors have to assume more extensive responsibilities apropos ensuring international peace and security in the virtual realm.

Through their technological expertise, ownership and resource structures, as well as international standing, private enterprises have the capacity to meaningfully contribute to the implementation of measures intended to increase international stability and security in the use of ICTs. They 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.

Synthesis

As is evident from the efforts introduced above, international norm-building is no longer the *domaine réservé* (reserved domain) of nation states but increasingly also the purview of business enterprises.[38] Private actors have been seen to extend their traditional zones of operation and engage in diplomatic dealings at the international level. In addition to their conventional functions as technology and service providers, infrastructure owners, brokers of technological expertise, and implementers of national and international commitments, they have come to assume roles as norm-proposers, and diplomatic change agents. [39]

And while there appears to be a general recognition, particularly among Western stakeholders, that issues concerning the security and stability of cyberspace cannot be addressed by sovereign actors alone, the norm-building activities of private sector entities raise a number of important follow-on questions pertaining to legitimacy and order. Some of these questions were addressed during the private sector expert panel as well as the private sector breakout session held on 1-2 November 2018 (please refer to **Private Sector Expert Panel – 1 November 2018**).

Meeting Report

The private sector expert panel convened on the first day of the Geneva Dialogue on Responsible Behaviour in Cyberspace consisted of four industry speakers, i.e. Evgeny Grigorenko (Kaspersky Lab), Jan Neutze (Microsoft), Miguel Sanchez (Telefonica), and Martin Dion (Kudelski Security), and ran for 90 minutes.

Private Sector Expert Panel – 1 November 2018

The discussions of the private sector exert panel were guided by eight key questions:

- What are the self-assigned/-perceived roles and responsibilities of different private sector actors in contributing to international peace, security and stability vis-à-vis the malicious use of cyberspace?
- In what ways are private sector actors seeking to promote more responsible behaviour within their own sector(s)? To what extent do these activities contribute directly (or indirectly) to the implementation of the UN GGE recommendations on norms and other international initiatives?
- How can the standards proposed by private sector actors be meaningfully enforced, and to what degree do they require the assistance of other actors? What do cooperative agreements pertaining to the enactment of standards of responsible behaviour in cyberspace look like?
- Where the attribution of the malicious use (or misuse) of ICT is concerned, is the relationship between state authorities (e.g. intelligence, investigation and enforcement agencies) and the private sector fully optimised?
- Is the private sector incentivised to contribute to the protection and security of critical infrastructure?

[38] Katja S Ziegler, 'Domaine Réservé' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2013) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398>.

[39] Scherer, Palazzo and Baumann (n 35); Jessica T Mathews, 'Power Shift' (1997) 76 Foreign Affairs 50 <https://www.jstor.org/stable/10.2307/20047909?origin=crossref>.

- Are state authorities fully open to collaboration with the private sector in the exercise of the state responsibility for security in/from cyberspace?
- How can the capacity of the private sector be more effectively exploited as far as responsible behaviour is concerned? Should private sector actors be acknowledged as cyberspace norm entrepreneurs in their own right, for example? If so, from where do they derive their legitimacy?
- Are there areas in which the private sector should not seek to be involved, i.e., are there roles and responsibilities which private sector actors should perhaps leave to others?

The expert panel discussion was brought underway by Jan Neutze (Microsoft) who argued that industry representatives have a key responsibility with regard to providing adequate levels of security to customers of relevant products and services. He also maintained that while security should be an overriding concern generally, one entity alone cannot address the burgeoning number of security concerns pertaining to the digital realm and that cooperation (among and outside of industry partners) is of the essence. To substantiate his point, Neutze elaborated on a number of Microsoft-led policy initiatives, including the Cybersecurity Tech Accord and the Digital Peace Now campaign which aim to foster joint efforts and greater awareness.

Addressing the question of what types of tools industry can provide to support responsible behaviour, Neutze held that naming and shaming as well as attribution assistance are thematic areas where private sector actors can contribute to the implementation of responsible behaviour. Additionally, Neutze said that private sector actors should have a systemic interest in protecting the digital environment given their roles as developers of products and providers of services. At the same time, he clearly held that the enactment of binding legal norms is the remit of governments.

Following Neutze, Martin Dion argued that it is critical to foster real (emphasis added) dialogue among different constituencies. He also cautioned that non-tech companies, especially those concerned with critical infrastructure, should be brought to the table. Employing a “realistic” lens, Dion warned that cybersecurity is not going to improve in the short term, and that more capacity-building (in particular with regards to critical infrastructure operators) and a true sense of shared responsibilities are needed.

In his presentation, Evgeny Grigorenko emphasised that there is a climate of mutual distrust and uncertainty among private and public sector entities and that in order to overcome this climate it is necessary to implement measures of accountability and transparency. According to Grigorenko, cybersecurity represents a global industry characterised by cross-border collaboration and competitiveness. In order to better understand the respective roles of governments, corporations, and civil society therein it is important to develop scalable frameworks of interaction, which help foster trust and credibility. As an example, Grigorenko cited Kaspersky Lab’s launch of a new transparency centre in Switzerland.

Grigorenko went on to argue that private sector entities have important roles to play with regard to direct user protection as well as resilience, and support of government-led initiatives.

Commending the remarks of his predecessors, Miguel Sanchez continued to underline the importance of infrastructure integrity and transparency, and highlighted Telefonica’s efforts in this regard (Telefonica’s Manifesto for a New Digital Deal). In Sanchez’ view, technology companies have a duty to respect and support governmental efforts directed at enhancing the security and stability of cyberspace. Citing Microsoft’s Cybersecurity Tech Accord, which Telefonica is a party to, Sanchez also highlighted the importance of industry collaboration.

Following the remarks by the four expert speakers, the panel proceeded to address questions and interjections from the audience. The questions posed and interjections made revolved around the following issue areas:

- The strategies employed by technology providers to guarantee assurance and deal with legacy technologies and digital infrastructures susceptible to attacks
- The propensity of private sector companies to name and shame other corporations
- The capacity and legitimacy of private sector entities to deal with normative topics
- The underlying motivations of private sector actors for launching initiatives pertaining to norms
- The willingness of private sector companies to contribute to (government-led) vulnerabilities equities processes
- The importance of private sector companies to act as interlocutors in international cybersecurity norms processes and the need for caution apropos heavy-handed and potentially innovation-curbing state-driven regulation
- The reporting on launched corporate initiatives
- The configuration/gathering of relevant private stakeholders and the importance of insurance companies
- The role of private sector entities in acts of active cyber defence

Responding to the issues raised, the four expert speakers echoed the importance of collaborative frameworks of interaction among governments and private sector entities, as well as the need to leverage existing institutional structures for exchange, such as the Global Forum for Cyber Expertise (GFCE) or the outcomes of processes such as the UN GGE. The experts also underlined the persisting demand for capacity-building efforts. Grigorenko, for example, maintained that in order to move from the recognition of issues to more actionable frameworks, three things are needed: better regulation (for both state and non-state actors), better technology, and more capacity building efforts.

Private Sector Breakout Session – 2 November 2018

The private sector breakout session that followed the private sector expert panel on the 2nd of November was made up of a mixed group of 15 participants from civil society, governments, and the private sector, and went on for 120 minutes. The breakout session was structured along three core components, a broadly-framed brainstorming session, a more targeted problem-analysis element, and a future oriented mind-mapping exercise. Participants were split into three sub-groups, and conducted three exercises in these configurations. The rationale behind splitting the group into smaller sub-groups was to allow for higher levels of diversity in terms of answers and outcomes.

Brainstorming

The first exercise focused on identifying extant roles and responsibilities of private sector actors vis-a-vis contributing to international peace and security in cyberspace. Overall, there was reasonable variation among the three sub-groups in terms of how private sector participants can and do contribute to responsible behaviour in cyberspace. The outcomes of the discussions held in the different subgroups are reported in tabular form below.

Brainstorming Outcomes What are the assigned and self-perceived roles and responsibilities of private sector actors in contributing to international peace, security, and stability vis-à-vis the malicious use of cyberspace?	
Group 1	Pursuing an idealistic approach, Group 1 identified three ideal-typical roles of private sector entities: - Proactive norm entrepreneurs (proposing norms) - Reactive norm implementers (especially with regard to the norms stipulated by the UN GGE) - Independent norm guardians (verifying whether there are violations of norms) - Norm enforcers (enabling and constraining behaviour based on norms) **Open question:** How can these different roles best be realised given the asymmetry of infrastructure ownership?
Group 2	Pursuing a more realistic approach, Group 2 maintained that private sector actors should: - Be more concerned with the protection of critical infrastructure - Devise and thoroughly test (security-deserving) products - Help governments respond to incidents and take on public risks **Open question:** It remains to be determined, who is addressing which risks?
Group 3	Without elaborating on specific roles, Group 3 held that it is not clear how responsibilities are allotted and distributed. **Open question:** Given the diversity of private sector actors, how can responsibilities best be identified and clarification be achieved?

Problem Analysis of Responsibilities

As part of the second exercise, breakout session participants were asked to address three different problem statements which resulted from the brainstorming activities of the first exercise. They then had to attend to each problem statement with five follow-up how-questions. The outcomes of the discussions held in the subgroups and answers to the relevant how-questions are reported in tabular form below.

Problem Statements					
Group 1	**Private sectors actors have to collaborate with other actors to implement the 2015 UN GGE norms.**				
	How?	How?	How?	How?	How?
	Dedicate threat information exchange required.	Clear defence/resilience protocols needed.	Joint response protocols required.	Multilateral alignment needed.	Dedicated scenario and stress testing required.

Group 2	**Private sector actors have to take on public risks.**				
	How?	How?	How?	How?	How?
	Clear risk definition and understanding needed.	Methodology to define security responsibilities required.	Expert body for definition of methodology needed.	—	—
Group 3	**Private sector roles and responsibilities are unclear.**				
	How?	How?	How?	How?	How?
	More granular differentiation of private sector actors needed (producers vs. operators vs. consumers)	Clear definition of responsibilities for each subcategory required (what is in, what is out).	Incentive structures for corporate baselines needed.	Accreditation and sanction schemes required to ensure compliance.	—

Mind-Map of the Future

The last exercise concentrated on identifying future roles of private sector actors with regard to contributing to responsible behaviour in cyberspace. The role profiles and possible future areas of activity devised are listed in tabular form below.

Mind-Mapping Exercise In what way should private sector actors contribute to the future of cyberspace, and how should their roles develop and change, respectively?	
Group 1	In order to address burgeoning numbers of cybersecurity incidents and foster responsible behaviour in cyberspace among non-state and state actors, Group 1 held that going forward, there need to be institutional structures supporting: - Shared rewards - Shared responsibilities - Shared risks Private actors were seen to be important players in shaping these configurations.
Group 2	Underlining the fact that a lot of work still has to be done in terms of identifying corresponding roles and responsibilities of private sector entities, Group 2 maintained that there is room for these actors to become: - Agents of harmonisation of standards - Creators of mutual transparency structures between public and private sector entities - Environment specific product developers (e.g. critical infrastructure)

Group 3	Group 3 focused their discussions on the need of private sector participants to act as drivers of collaboration and inciters of mutual exchange. To that end the future roles were identified to be: - Shapers of collaborative arrangements (among groups of like-minded entities) - Enforcers of cross-referencing security accreditation schemes

Overall, the discussions during the breakout session were open and transparent and benefitted from the inputs of preceding conversations and panels.

Conclusion

As private sector actors continue to be concerned about "the immediate and future threats to their critical services and infrastructures, [resulting] from the misuse of information and communications technologies," and seek diplomatic engagement, it is important to reconsider existing forms of interaction and cooperation among governmental and non-governmental entities.[40] The norm-building activities of private sector actors point to a need for more collaborative forms of governance, in which business enterprises participate in joint steering efforts with sovereign authorities.

The results of the private sector expert panel as well as the breakout session evidenced that, "it is time to go beyond sharing and ad hoc cooperation, to collaboration at scale across borders, stakeholders, and sectors."[41] In order to move from cyber insecurity to cyber stability, it is critical that traditional law-based systems interact with private sector actors and their norms-based systems in a symbiotic way, and responsibilities are pooled accordingly.[42]

The enactment of peace and security in the virtual realm requires governance setups with greater legislative, administrative, and adjudicatory flexibility, consisting of both public and private entities.[43] "Failure to recognise the role of private governance in public policymaking is to risk losing some of its contributions to providing high-level expertise needed for intelligent policymaking today, responsiveness to technological change, networks to reduce the global governance gap, and alternatives to the state."[44]

[40] Melissa Hathaway in Fen Osler Hampson and others, 'Getting Beyond Norms: New Approaches to International Cyber Security Challenges' (2017) 5 <https://www.cigionline.org/sites/default/files/documents/Getting Beyond Norms.pdf>.

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

[42] Larry Catá Backer, 'Private Actors and Public Governance Beyond the State: The Multinational Corporation, the Financial Stability Board, and the Global Governance Order' (2011) 18 Indiana Journal of Global Legal Studies 101.

[43] Daniel Bodansky, *Legitimacy* (Daniel Bodansky, Jutta Brunnée and Ellen Hey eds, Oxford University Press 2008) 4 <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199552153.001.0001/oxfordhb-9780199552153-e-30>.

[44] Louise Marie Hurel and Luisa Cruz Lobato, 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs' [2018] Journal of Cyber Policy 1, 5.

Bibliography

Austin G, McConnell B and Neutze J, ‘Promoting International Cyber Norms: A New Advocacy Forum’ (2015) <https://cybersummit.info/sites/cybersummit.info/files/BGCyberNorms_FINAL.pdf>

Björkdahl A, ‘Norms in International Relations: Some Conceptual and Methodological Reflections’ (2002) 15 Cambridge Review of International Affairs 9 <http://www.tandfonline.com/doi/full/10.1080/09557570220126216>

Bodansky D, *Legitimacy* (Daniel Bodansky, Jutta Brunnée and Ellen Hey eds, Oxford University Press 2008) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199552153.001.0001/oxfordhb-9780199552153-e-30>

Catá Backer L, ‘Private Actors and Public Governance Beyond the State: The Multinational Corporation, the Financial Stability Board, and the Global Governance Order’ (2011) 18 Indiana Journal of Global Legal Studies 101

Charney S and others, ‘From Articulation to Implementation: Enabling Progress on Cybersecurity Norms’ (2016) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8>

Chong J, ‘U.S. Cybersecurity: Why Is Software So Insecure?’ (*The New Republic*, 2013) <https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure> accessed 12 September 2018

Condon S, ‘Google Pitches New Legal Framework for Cross-Border Data Handling’ (*ZDNet*, 2017) <https://www.zdnet.com/article/google-pitches-new-legal-framework-for-cross-border-data-handling/> accessed 19 July 2018

Cybersecurity Tech Accord, ‘Cybersecurity Tech Accord’ (2018) <https://cybertechaccord.org/accord/> accessed 10 July 2018

Finnemore M, ‘Cybersecurity and the Concept of Norms’ (2017) <http://carnegieendowment.org/files/Finnemore_web_final.pdf>

Finnemore M and Hollis DB, ‘Constructing Norms for Global Cybersecurity’ (2016) 110 The American Journal of International Law 425 <http://www.jstor.org/stable/10.5305/amerjintelaw.110.3.0425>

Finnemore M and Sikkink K, ‘International Norm Dynamics and Political Change’ (1998) 52 International Organization 887 <http://journals.cambridge.org/abstract_S0020818398440608>

Haas M, ‘We Need a New Digital Deal So That Everyone Benefits From Digitalisation’ (*Telefónica*, 2018) <https://www.telefonica.de/fixed/news/6135/article-by-ceo-markus-haas-we-need-a-new-digital-deal-so-that-everyone-benefits-from-digitalisation.html> accessed 11 July 2018

Hampson FO and others, ‘Getting Beyond Norms: New Approaches to International Cyber Security Challenges’ (2017) <https://www.cigionline.org/sites/default/files/documents/Getting Beyond Norms.pdf>

Healey J, ‘Innovation on Cyber Collaboration: Leverage at Scale’, vol 1 (2018) <http://www.atlanticcouncil.org/images/publications/Innovation-Cyber-WEB.pdf>

Hern A, ‘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> accessed 6 February 2018

Hinck G, ‘Private-Sector Initiatives for Cyber Norms: A Summary’ (*Lawfare*, 2018) <https://www.lawfareblog.com/private-sector-initiatives-cyber-norms-summary> accessed 25 June 2018

Hurel LM and Lobato LC, ‘Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs’ [2018] Journal of Cyber Policy 1

Hurwitz R, 'The Play of States: Norms and Security in Cyberspace' (2014) 36 American Foreign Policy Interests 322 <http://www.tandfonline.com/doi/abs/10.1080/10803920.2014.969180>

Kaeser J, 'Working Together for More Security in the Digital World' (*LinkedIn Pulse* , 2018) <https://www.linkedin.com/pulse/working-together-more-security-digital-world-joe-kaeser> accessed 3 August 2018

Kavanagh C, 'The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the the 21th Century' (2017) <http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf>

Kurucz EC, Colbert BA and Wheeler D, *The Business Case for Corporate Social Responsibility*, vol 1 (Andrew Crane and others eds, Oxford University Press 2009) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199211593.001.0001/oxfordhb-9780199211593-e-004>

Mathews JT, 'Power Shift' (1997) 76 Foreign Affairs 50 <https://www.jstor.org/stable/10.2307/20047909?origin=crossref>

Maurer T, 'Cyber Norm Emergence at the United Nations' (2011) <http://belfercenter.hks.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf> accessed 20 February 2018

Maurer T and Taylor K, 'Outlook on International Cyber Norms: Three Avenues for Future Progress' (*Just Security*, 2018) <https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/> accessed 9 July 2018

McKay A and others, 'International Cybersecurity Norms' (2014) <https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/>

Microsoft, 'Five Principles for Shaping Cybersecurity Norms' (2013) <https://www.microsoft.com/en-us/cybersecurity/content-hub/five-principles-for-shaping-cybersecurity-norms>

——, 'Digital Peace Now' (2018) <https://digitalpeace.microsoft.com/#dp-share> accessed 4 December 2018

Microsoft Security Response Center, 'Announcing Coordinated Vulnerability Disclosure' (*TechNet*, 2010) <https://blogs.technet.microsoft.com/msrc/2010/07/22/announcing-coordinated-vulnerability-disclosure/> accessed 8 August 2018

Radu R, 'Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace' in Jan-Frederik Kremer and Benedikt Müller (eds), *Cyberspace and International Relations* (Springer Berlin Heidelberg 2014) <http://link.springer.com/10.1007/978-3-642-37481-4>

Risse-Kappen T, Ropp SC and Sikkink K, *The Power of Human Rights: International Norms and Domestic Change* (Cambridge University Press 1999)

Sandholtz W, 'International Norm Change' (2017) 1 Oxford Research Encyclopedia of Politics 1 <http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-588>

Scherer AG, Palazzo G and Baumann D, 'Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance' (2006) 16 Business Ethics Quarterly 505 <https://www.cambridge.org/core/product/identifier/S1052150X00011040/type/journal_article>

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> accessed 11 July 2018

——, 'Time for Action: Building a Consensus for Cybersecurity' (*Cybersecurity*, 2018) <https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html> accessed 3 July 2018

Smith B, ‘A Digital Geneva Convention to Protect Cyberspace’ (2017) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH>

——, ‘The Need For a Digital Convention’ (*Microsoft*, 2017) <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv> accessed 9 July 2018

——, ‘34 Companies Stand Up for Cybersecurity with a Tech Accord’ (*Microsoft*, 2018) <https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/> accessed 10 July 2018

Stevens T, ‘A Cyberwar of Ideas? Deterrence and Norms in Cyberspace’ (2012) 33 Contemporary Security Policy 148 <https://www.tandfonline.com/doi/full/10.1080/13523260.2012.659597>

Telefónica, ‘A Digital Manifesto: An Open and Safe Internet Experience For All’ (2014) <https://www.telefonica.com/documents/341171/362460/20140410_A_Digital_Manifesto_ING_FINAL_reviewed.pdf/978031f0-d352-4f65-9c3c-b7d70fddf407>

——, ‘A Manifesto for a New Digital Deal’ (2018) <https://www.telefonica.com/digital-manifesto/assets/a_manifiesto_for_a_new_digital_deal.pdf>

Tonello M, ‘The Business Case for Corporate Social Responsibility’ (*Harvard Law School Forum on Corporate Governance and Financial Regulation*, 2011) <https://corpgov.law.harvard.edu/2011/06/26/the-business-case-for-corporate-social-responsibility/#8b> accessed 18 July 2018

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (2010) <http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201>

——, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (2013) <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>

——, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ (2015) <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>

United Nations Human Rights Council, ‘Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression’ (2018) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>

Väljataga A, ‘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> accessed 5 July 2018

Walker K, ‘Digital Security and Due Process: A New Legal Framework for the Cloud Era’ (*Google*, 2017) <https://www.blog.google/outreach-initiatives/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/> accessed 5 July 2018

——, ‘Digital Security and Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era’ (2017) <https://www.blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf>

Ziegler KS, ‘Domaine Réservé’ in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2013) <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398>