Unpacking the GGE's framework on responsible state behaviour: Cyber norms

At the UN First Committee, two processes—the UN Group of Governmental Experts (GGE) and the Open-ended Working Group—are currently exploring the same question: responsible state behaviour in cyberspace. This term comes from a 2015 report by the previous GGE, which defines it according to a framework of four components: 1) norms, rules and principles; 2) confidence-building measures; 3) capacity-building; 4) the application of international law in cyberspace.

Understanding these components is crucial to engaging effectively at the GGE and OEWG. In this series, we'll be looking at each component in turn—looking at what they mean, how they have been defined, and their relevance to human rights. In this entry, we examine norms in cyberspace, or "cyber norms". This explainer was authored by Deborah Brown and Anriette Esterhuysen of the Association for Progressive Communications and Sheetal Kumar of Global Partners Digital.

Defining norms in cyberspace

Norms

Norms are commonly defined as socially enforced rules or expectations: like "give your seat up to the less abled on public transport" or "don't make noise in a cinema".[1] They establish a collective expectation for the appropriate behaviour of specific actors, which makes them valuable as policy tools, as they help clarify responsibilities and create obligations. Norms can be developed through bilateral agreements, or by groups of states or other actors. They can be "declared" unilaterally or they can evolve through practice by states or other actors.

Norms are different from (but tied to) related concepts, such as principles and laws. Principles reflect the values and vision of a specific group or institution, but don't identify what actions specific actors need to perform to achieve a stated goal, even when they describe in broad terms the obligations of these actors.[2] Norms, on the other hand, are more specific and link actors to specified expected behaviour. In that sense, they trigger more active accountability than principles do.[3] Norms can, over time, be codified into laws, at which point they become binding. However, laws which codify norms which are not widely shared are more difficult to enforce, and are therefore more likely to be broken.

Cyber norms and the GGEs

Cyber norms are, put simply, norms that apply to cyberspace. However, as there is no agreement on a definition of cyberspace, cyber norms also have no precise definition. In practice, however, they refer to how actors should or should not behave with regard to their use of information and communication technologies (ICTs).

As mentioned earlier, norms can be codified into laws or legally binding measures over time and this can help with compliance, particularly in contexts where the rule of law is strong. Conversely, unless the norms are widely shared and accepted, codifying them in laws can be ineffective. In cyberspace, given the dynamic nature of technological developments and the lack of agreement on how existing regulatory frameworks and commitments—like international law—apply, non-binding norms can plug gaps in regulatory and legal frameworks. However, cyber norms have not developed in a vacuum, delinked from understandings of existing legal commitments. Rather, norm building efforts have played a role in fostering common understandings of existing commitments in a new context.

The most robust multilateral discussion on norms in cyberspace has evolved in the UN General Assembly's First Committee's Groups of Governmental Experts (GGE),[4] which has referred to norms as having "the potential to strengthen common understandings and act as "an essential measure to reduce risks to international peace, security and stability".[5]

In 2010, the GGE first recognised the need for norms on state use of ICTs to reduce collective risk and protect national and international infrastructure, and recommended dialogue among states on norms. However, it fell short of recommending any specific norms.[6] It wasn't until 2013 that member states moved to recommend some specific norms derived from international law:

- That state sovereignty applies to how states conduct ICT-related activities and to their jurisdiction over ICT infrastructure within their territory;[7]
- That state efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms;[8]
- That states must not use proxies to commit

> internationally wrongful acts and must ensure that their territories are not used by non-state actors for unlawful use of ICTs.[9] [10]

The GGE's stance on norms was further elaborated at its fourth iteration in 2015, which stated that norms "reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States."[11] Most of the recommendations from 2013 found their way into the 2015 report alongside 11 voluntary, non-binding norms.

Though voluntary and non-binding, these norms are concrete in their nature: they specify what behaviour is expected of state actors in specific contexts, and either suggest "positive" actions states should undertake or "negative" ones they should refrain from. We look at each of the GGE 2015 norms in more detail in section 3.

The evolution of the discussion on norms by GGEs

- 2010: Recognises the need for norms and recommends dialogue among states to discuss norms.
- 2013: Makes recommendations on norms, rules and principles, and concludes that some norms can already be derived from existing international law.
- 2015: Agrees on 11 specific voluntary, non binding norms for responsible behaviour of state, aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.

Following their adoption by the General Assembly, the 11 norms have been endorsed by other bodies, including the Group of Seven (G7),[12] the Group of 20 (G20),[13] the Organization for Security and Cooperation in Europe (OSCE),[14] and the Association of Southeast Asian Nations (ASEAN).[15] They are also referred to and supported by multistakeholder initiatives such as the Paris Call for Trust and Security in Cyberspace[16] and by the Global Commission on the Stability of Cyberspace.

The current situation and trends

The GGE report in 2015 was adopted by the General Assembly, which called on every member state to be "guided" in its use of ICTs by the recommendations included in the report.

When it comes to the 11 non-binding norms of the UN GGE, there is now general agreement that the most important next step is for these norms to be applied and for compliance to be monitored. Although they've been endorsed by all member states, they will be ineffective in achieving their stated objective to "strengthen common understandings to increase stability and security in the global ICT environment" if states do not implement them. One way that norms can be implemented is through national strategy documents, like cybersecurity strategies, and/or through regional frameworks. They could also be monitored through a global-level mechanism such as a peer review process, or through states reporting to an international process. As of now, no such mechanism yet exists.

So far, the government of Australia has published a report on the status of its implementation of the GGE norms, and the ASEAN Regional Forum is developing a framework for assessing the status of compliance among its member states with the GGE norms. The G7 also reportedly conducted an assessment of its members' implementation of GGE norms. However, the status of norm implementation remains uneven, and difficult to ascertain. Some multistakeholder initiatives such as the Global Forum on Cyber Expertise and the Internet Governance Forum's Best Practice Forum have sought to address this lack of clarity on norm implementation, and have carried out research to assess the implementation of both the GGE norms and the other normative proposals outlined above, although this research remains preliminary.

There are a number of challenges when it comes to implementing the norms:

- Varied understandings or definitions of the key terminology referred to in the norms (e.g critical infrastructure);
- Varied levels of awareness of the existence of the norms among states and among other stakeholders, as well as in capacity to implement them;
- The difficulty of tracing and attributing incidents in cyberspace;
- The flouting of norms by influential states, which acts as a disincentive for others to comply with them;
- A lack of clear institutional mechanisms or processes to monitor and report on compliance.

Finally, in the absence of a binding framework, and given the voluntary nature of the current GGE norms, their implementation will rely on political will. Only a belief by states that they have a vested interest will push them to allocate the necessary resources to implement the norms, share their experiences, and hold each other accountable.

The 2015 GGE report also recognises that there may be a need to develop new norms in the future. However, this is currently a source of

The current situation and trends (cont'd)

disagreement among states, as some consider the current set of norms sufficient, and others believe that—until there is compliance with current norms—there is no point in developing further ones. There is also disagreement about the role of different actors in both developing and implementing norms. In this context, characterised by a slow uptake of the GGE norms, the multistakeholder nature of the governance of the internet, and a lack of agreement among states on whether new norms are needed, a range of other norm building efforts have emerged alongside the UN processes.

Examples include:

- Freedom Online Coalition (FOC)'s Free and Secure Recommendations,[17] a set of 13 "normative" recommendations designed to raise the profile of human rights as an integral consideration in cybersecurity policymaking, which were developed by a multistakeholder working group and endorsed by FOC member governments.
- Global Commission on the Stability of Cyberspace (GCSC)[18], a multistakeholder initiative which has put forward a framework, principles, and eight norms to help foster responsible state and non-state behavior in cyberspace. These norms are intended to be complementary to norms developed within the context of the UN.
- Paris Call for Trust and Security in Cyberspace[19], initiated by the government of France and endorsed by 67 states and hundreds of other institutions, from business to civil society and the academic and technical sectors. The Call affirmed the importance of voluntary norms of responsible state behavior to cybersecurity, drawing on the 2015 GGE norms and the GCSC norms.
- Private sector initiatives such as Microsoft's Cybersecurity Tech Accord[20], Siemens's Charter of Trust[21], and Kaspersky Lab's Global Transparency initiative[22]. These industry-led norms lay out voluntary measures that private actors agree to take to protect cyberspace and their users and customers from cyber threats while using their products and services.

Both the OEWG and GGE discussions will address the implementation of the GGE norms. And, as the OEWG mandate includes "the possibility of introducing changes to them or elaborate additional rules of behaviour", it will likely discuss the need for new norms to be adopted.

The link between cyber norms and human rights

The link between cyber norms and human rights may not be immediately obvious. But their goal of promoting responsible state behaviour in cyberspace contributes to the underlying conditions that are needed for the exercise of human rights today.

People increasingly rely on the availability, integrity and confidentiality of information and its underlying infrastructure to exercise their rights. If states are engaging in internationally malicious acts—and, as a result, making the internet (and the applications and devices dependent on it) less stable and secure—human rights can be threatened. For example, by stockpiling vulnerabilities or inserting backdoors into ICT software or hardware, states can make it easier for malicious hackers to gain access to personal communications and metadata. This can violate a range of rights, including privacy. In addition, by attacking and damaging critical infrastructure, states can violate a number of human rights, including the rights to life, health, and security, and to participate in elections. If, by contrast, states work to ensure the security of their critical infrastructure, they can safeguard these rights. In addition, as mentioned previously, cyber norms are derived from and refer to international law, which includes international human rights law, and require states to respect their obligations under them. Human rights mechanisms, in particular the UN Special Procedures, have interpreted international human rights law in light of technological developments, which can inform the implementation of cyber norms. While international human rights law provides a guiding framework, cyber norms can go further in helping to foster a shared understanding of how to respect human rights in the context of cyberspace.

The implementation of cyber norms and the role of human rights defenders

As the GGE norms were negotiated in a closed space, and only among states, the wide range of issues at stake—and the roles of non-state actors in their effective implementation—may not have been adequately considered. For example, norm (k) refers only to "authorized emergency response teams", whereas a number of emergency response teams are non-governmental, or private, and also require protection.

Yet, because the norms were agreed and adopted by consensus at the General Assembly, renegotiating them would be detrimental to their implementation. A more effective way forward would be for the GGE norms to be

The link between cyber norms and human rights (cont'd)

implemented and monitored by a wide range of stakeholders, including human rights defenders (HRDs).

There are, however, a number of challenges that HRDs face in trying to leverage the GGE cyber norms as tools in their work, including in monitoring state compliance. Until recently, most HRDs did not pay much attention to cyber norms, which is understandable considering there were very few opportunities for HRDs to engage with cyber norm discussions.

The link between human rights and cyber norms is not necessarily clear. Besides one norm that directly references human rights, they are not written in a way that directly unpacks the implications for human rights. But cyber norms are not currently effectively enforced by states themselves—and, just as with human rights, constant monitoring and pressure from watchdogs is needed for states to comply with cyber norms in an inclusive and human-rights respecting way.

For HRDs to play an effective role in monitoring and advocacy around the implementation of the GGE norms that have already been adopted, they need to be aware of norms, the contexts from which they have emerged (and in which they are intended to be applied), and to understand their relevance for human rights.

Each norm has an impact on human rights; albeit some more directly than others. The implementation of each norm can result in a negative or beneficial impact on human rights, and it is therefore important for HRDs to engage, either in directly implementing the norms or in monitoring their implementation.

Note: in this section of this brief, the content of each norm is unpacked with a particular focus on its relevance for human rights, and how its implementation can impact human rights—with opportunities for HRDs to engage in the implementation. As norms (e)(f) and (h) are closely related, they have been combined for the purposes of the analysis and commentary below.

What do the 11 GGE cyber norms mean for human rights?

> *(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.*[23]

The first action requested of this norm is for states to, in cooperation with one another, develop and apply measures to increase stability and security in the use of ICTs. This is critical for the enjoyment of human rights in the digital age. As more people and devices are connected, the stability and security of ICTs affects virtually every human right, from the right to freedom of expression, association, and assembly and the right to privacy, to economic, social and cultural rights (like the right to health, work and education).

Even those who are not yet online rely on secure infrastructure to access the provision of public services. However, there is a lack of understanding among states that the same measures that promote and protect human rights online also increase stability and security in the use of ICTs. For example, strong encryption supports the enjoyment of human rights, in particular the rights to privacy, freedom of expression and freedom of peaceful assembly and association, but it is also essential in protecting data and networks from attack.

The second action requested by this norm—to prevent ICT practices that are acknowledged to be harmful—can be interpreted as including the prevention of internet shutdowns, arbitrary surveillance, government hacking, censorship, and cyber attacks on HRDs.[24] However, states often initiate these practices themselves in the name of "security". This is inconsistent with what states have committed to through UN Human Rights Council (UN HRC) resolutions, which call on all states "to address security concerns on the Internet in accordance with their international human rights obligations to ensure the protection of all human rights online [...] in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development".[25]

It is therefore important that HRDs monitor state practice to ensure that whatever measures states employ "to increase stability and security in the use of ICTs" do not result in practices which are harmful. This ties closely with norm (e), where HRDs have an essential role to play.

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

This norm is intended to reduce escalation of tensions from misattribution of cyberattacks. Requiring that all relevant information is taken into consideration should help guard against the escalation of tensions in cyberspace. This is in the interest of HRDs, because the escalation of tensions between states can harm human rights by leading to increased cyber attacks, which can reduce access to essential services and compromise the integrity of sensitive and personal data. In calling for all relevant information to be considered, it is critical for states to work inclusively with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of human rights.

*

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

This norm refers to the law of state responsibility and the principle of due diligence, which—under international law—obliges a state to not knowingly allow its territory to be used for acts contrary to the rights of other states.

It can also be read to refer to the principle under international human rights law that states must protect against human rights abuses within their territory and/or jurisdiction by third parties, including business enterprises. For the prevention of internationally wrongful acts by third parties, states need to be far more transparent and willing to share information about abuses by private actors. They also need to be willing to hold private actors who enable or facilitate these acts to account. HRDs can play a role here by monitoring and reporting these abuses.

*

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

While cooperation among states to counter of the use of ICTs for terrorist and criminal purposes is of critical importance, such efforts should not include disproportionate responses that violate human rights. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism concluded, in a recent report, that a number of states have made use of broad invocations of the need to protect national security, counter terrorism and prevent violent extremism, to restrict rights and close civic space.[26] The same report highlights that information sharing in the name of countering terrorism has also resulted in violations of the right to privacy, due process, and non-discrimination. Therefore, to ensure these processes are subject to oversight and accountability that protect human rights, it is important for HRDs to be more aware of efforts by law enforcement and businesses to address cybercrime and terrorists' use of ICTs.

*

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

The UN HRC and General Assembly have passed numerous resolutions over the last few years that provide guidance on how to safeguard human rights while reinforcing security and stability online. HRDs can use these in advocating for human rights-respecting approaches to cybersecurity. For example, regarding encryption, they have recognised the importance of technical solutions to secure and protect the confidentiality of digital communications, including measures around encryption and anonymity, for ensuring the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association.[27] For the internet to remain global, open and interoperable, it is imperative that states address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of opinion and expression, freedom of association and privacy.[28]

UN resolutions have also called on states to refrain from employing unlawful or arbitrary surveillance techniques, including forms of hacking,[29] noting that, while concerns about public security may justify the gathering and protection of certain sensitive information, states should ensure full compliance with their obligations under international human rights law in their collection of this sensitive information.

Finally, UN HRC and UNGA resolutions have encouraged all states to promote an open, secure, stable, accessible and peaceful ICT environment, based on respect for international law, including the obligations enshrined in the Charter of the United Nations and human rights instruments.[30]

Human rights defenders can play a wide range of roles here—by shaping policies, building the capacity of stakeholders to implement frameworks for the national context in a rights respecting manner, providing technical and policy solutions to existing challenges, and raising awareness of existing initiatives and commitments. Human rights defenders can also play a role in monitoring state practice at the national level, including through research, and using regional mechanisms (where possible), and mechanisms at the global level, in particular the UN HRC, to highlight both good practice and violations of human rights. The research and advocacy work conducted by HRDs in this regard plays an essential role in promoting compliance with the human rights commitments referred to in this norm.

*

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

There is no single definition of "critical infrastructure" but it is usually understood to refer to objects, systems and networks that are critical to the functions or provision of public services like transport, water and wastewater systems, food and agriculture, electricity, financial services and telecommunications. The protection of these systems is important for human rights, as the ability to communicate, access information, and share information about rights violations is critical.

While these norms focus on the role of states, the resolution on the creation of a global culture of cybersecurity and the protection of critical information infrastructures[31] specifically mentions cooperation among all stakeholders. It also recognises that “efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation.'' HRDs can work with states and the technical community to ensure that they are taking the measures necessary to protect critical infrastructure that they rely on for the enjoyment of human rights. The resolution has an Annex on “Elements for protecting critical information infrastructures” that may be useful for HRDs to refer to.

*

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

Confidence in the security of ICT products is critical for the exercise of a range of human rights. In addition to being necessary for the exercise of freedom of expression, the right to privacy and other civil and political rights, being able to use ICT products securely may also be necessary for the right to work, given how many people rely on the secure use of ICTs for their livelihood.

Ensuring the integrity of the supply chain requires that states refrain from mandating backdoor access to ICT products (hardware and software) and, crucially, in popular communication platforms. Additionally, this norm is about preventing the proliferation of malicious ICTs and techniques. Malicious ICTs and techniques don’t just put everyone’s security at risk—they are also often exploited by state and non-state actors alike to target and attack HRDs. Research from civil society and academia has documented how malware and software vulnerabilities which are used to target HRDs have been disseminated through app stores and software updates.[32]

HRDs can play a role here, in supporting all stakeholders in the supply chain to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. HRDs have already played an essential role in other fields, such as the extractive industries,[33] in defending human rights in supply chains by developing tools such as “human rights impact assessments”, and in monitoring compliance with human rights standards.[34] They have also recently developed a tool for assessing the human rights impact of internet registries.[35]

A number of ICT companies, including Ericsson, Telefonica and Vodafone, have developed human rights policies and commitments, which HRDs can monitor, and propose recommendations for improvement. Further, countries' National Action Plans on Business and Human Rights (NAPs) are an important tool for supporting integrity and security of ICT products. Civil society organisations can work together with governments to develop NAPs which support responsible state practice with regards to ICTs.[36]

*

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

The GGE report does not define vulnerabilities in any particular way, but—according to one definition—they can be described as "a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy" (IETF). Related to the above norm, responsibly reporting on ICT vulnerabilities (which in some cases have been the main mechanism deployed in cyberattacks) is essential. Vulnerabilities have been used to attack critical infrastructure, with extremely damaging effects, such as Stuxnet.[37]

A recent report into current practices on vulnerability disclosure suggested protecting security researchers and clearly outlining the roles and responsibilities of all stakeholders, including vendors, in reporting processes.[38]

Human rights defenders can ensure that processes for responsible state disclosure exist, that they do not criminalise security researchers, and that they are in line with best practice.[39]

*

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Computer emergency response teams (CERTs) are the first line of response to a cyber attack. They may be affiliated with a state, or be independently run by a private sector entity or civil society organisation. Computer Incident Response Center for Civil Society, or CiviCERT, is a network of CERTs, Rapid Response teams, and independent internet content and service providers, who help civil society prevent and address digital security issues.[40] Some of its members are civil society organisations such as Access Now, Amnesty International, Defend Defenders, Frontline Defenders, Fundacion Karisma, and Human Rights Watch.

Importantly, this norm does not refer to a national CERT, but a CERT "of another State". Even though it's not clear whether this can be understood to provide protection of all CERTs (as it refers only to "authorized" entities), it is important that all CERTs and their networks are aware of this norm, and support its implementation.

Where CERTs do not yet exist, civil society and human rights defenders can advocate for their establishment in a manner that is inclusive, and ensures they are independent and operate with transparency. Incident response requires quick information sharing, which is dependent on strong relationships between the actors involved. A degree of independence and transparency between CERTs and parts of government is important from a rights perspective, to ensure that a CERT carries out its work without impinging on freedom of expression or privacy.[41]

Endnotes

1. From the introduction to “Norms” by Christine Horne in the Oxford Bibliographies. https://www.oxfordbibliographies.com/view/document/obo-9780199756384/obo-9780199756384-0091.xml
2. Cybersecurity and the concept of norms by Martha Finnemore, Carnegie Endowment for International Peace, November 30, 2017. https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870
3. Ibid (Finnemore, 2017)
4. Since 2004, UNGA has established five Groups of Governmental Experts (GGE) to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed. Over the years GGEs have focused on existing and emerging threats, how international law applies in the use of ICTs, norms, rules and principles of responsible behavior of States, confidence-building measures, and capacity building. For more information on the GGEs, see: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf
5. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013) Section III, p7 https://undocs.org/A/70/174
6. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 30 July 2010. https://undocs.org/A/65/201
7. This recommendation was included in the 2015 GGE report under the section of how international law applies to the use of ICTs. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Section VI. July 2015 https://undocs.org/A/70/174
8. The 2015 GGE report builds on this in its recommendations and in the section on international law (para 26).
9. This recommendation appears verbatim in the international law section of the 2015 report. Para 28 (e)
10. Fact sheet: Developments In The Field Of Information and Telecommunications In The Context Of International Security, UNODA, July 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf
11. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015) Section III, p7 https://undocs.org/A/70/174
12. G7 Principles and Actions on Cyber, https://www.mofa.go.jp/files/000160279.pdf
13. 2015 G20 Leaders' Communiqué, http://www.g20.utoronto.ca/2015/151116-communique.html
14. https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/OSCE+-Confidence+Building+Measures+to+Reduce+the+Risk+of+Conflict+Stemming+-from+the+Use+of+Information+and+Communication+Technologies+2016+3-10-20-16.pdf
15. 2nd ASEAN Cyber Norms Workshop, https://ict4peace.org/activities/policy-research/policy-research-cs/2nd-asean-cyber-norms-workshop-in-singapore-supported-by-ict4peace
16. Paris Call for Trust and Security in Cyberspace. 12 November 2018. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf
17. https://freeandsecure.online/
18. https://cyberstability.org/
19. 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
20. Microsoft Tech Accord, https://cybertechaccord.org/
21. Siemens Charter of Trust, https://new.siemens.com/global/en/company/stories/research-technologies/cybersicherheit-charter-of-trust.html
22. Global Transparency Initiative, https://www.kaspersky.com/about/press-releases/2017_trust-first-kaspersky-lab-launches-its-global-transparency-initiative
23. This and the subsequent norms are from paragraph 13 of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015) Section III, p7 https://undocs.org/A/70/174
24. UN Human Rights Council Resolution on “the Promotion, Protection, and Enjoyment of Human Rights on the Internet” (A/HRC/RES/38/7) https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/7, UN Human Rights Council Resolution on “the safety of journalists” (A/HRC/RES/39/6) http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/39/6, UN General Assembly Resolution on “the Right to Privacy in the Digital Age” (A/RES/73/179) https://undocs.org/en/A/RES/73/179
25. UN Human Rights Council Resolution on “the Promotion, Protection, and Enjoyment of Human Rights on the Internet” (A/HRC/RES/38/7) https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/7

Endnotes (cont'd)

26. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/40/52
27. HRC res 38/7
28. Ibid.
29. UNGA res 73/179
30. Ibid.
31. https://undocs.org/en/A/RES/58/199
32. Amnesty International, https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/; Citizen Lab, https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/
33. https://www.hrw.org/report/2018/02/08/hidden-cost-jewelry/human-rights-supply-chains-and-responsibility-jewelry
34. https://www.business-humanrights.org/
35. https://www.article19.org/resources/assessing-human-rights-impacts-internet-registries/
36. https://globalnaps.org/issue/information-communications-technology-ict-electronics/
37. https://en.wikipedia.org/wiki/Stuxnet
38. https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/
39. The Global Commission on the Stability of Cyberspace has two norms that addresses vulnerabilities, including one that proposes the establishment of vulnerability equity processes (VEPs). https://cyberstability.org/norms/#toggle-id-5
40. https://www.civicert.org/
41. The need for CERTs to be independent is also addressed in the GPD briefing on capacity building (part of the same series as this briefing on norms). https://www.gp-digital.org/wp-content/uploads/2019/10/RSB-1_CCB_export__FINAL.pdf