IGF 2020

Best Practice Forum on Cybersecurity

Exploring Best Practices
in relation to
International Cybersecurity Agreements

BPF Final output document

December 2020

Acknowledgements

The *Best Practice Forum Cybersecurity (BPF)* is an open multistakeholder effort conducted as an intersessional activity of the *Internet Governance Forum (IGF)*. This report is the final output of the IGF 2020 BPF on Cybersecurity and is the product of the collaborative work of many:

BPF Cybersecurity coordinating team

Ben Wallis, *MAG Co-facilitator*
Markus Kummer, *BPF Co-faclilitator*
Maarten Van Horenbeeck, *BPF Lead expert*
Wim Degezelle, *BPF Consultant*

Mallory Knodel, *BPF Workstream Lead*
John Hering, *BPF Workstream Lead*
Sheetal Kumar, *BPF Workstream Lead*

Key contributors

Anastasiya Kazakova
Apratim Vidyarthi
Ayesha Khan
Carina Birarda
Frans van Aardt
Louise Marie Hurel
YingChu Chen

Formal contributions submitted to the BPF Cybersecurity:
Australian Strategic Policy Institute ASPI, Duncan Hollis, EastWest Institute, Global Commission on the Stability of Cyberspace GCSC, Tim Maurer.

Participants to the discussions on the BPF mailing list and virtual meetings

Panelists and Participants to the BPF Cybersecurity session at the virtual IGF 2020:
Panelists: Aude Gery, GEODE; Anastasiya Kazakova, Kaspersky; Apratim Vidyarthi, University of Pennsylvania Law School; Isaac Morales, Government of Mexico; John Hering, Microsoft; Louise Marie Hurel, Igarapé Institute; Maarten Van Horenbeeck, First; Moliehi Makumane, Government of South Africa; Pablo Hinojosa, APNIC; Sheetal Kumar, Global Partners Digital; Sherif Hashem, SUNY Polytechnic Institute; Stéphane Duguin, CyberPeace Institute.

Disclaimer:

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

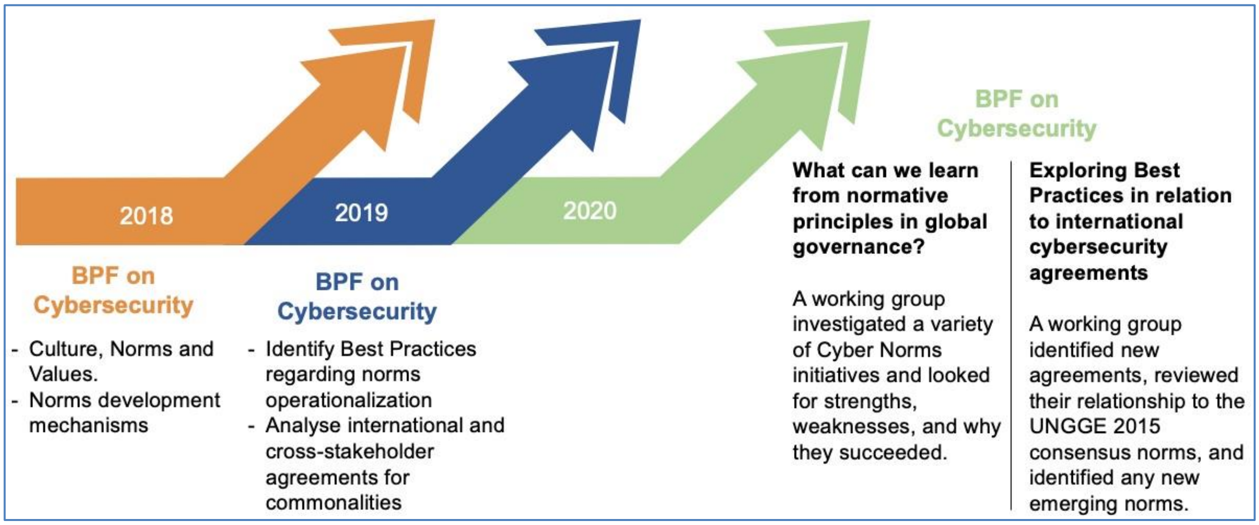
Executive summary

Introduction to the work of the BPF Cybersecurity in 2020 and key takeaways

Introduction to the work of the BPF Cybersecurity in 2020

To enrich the potential for Internet Governance Forum (IGF) outputs, the IGF has developed an intersessional programme of Best Practice Forums (BPFs) intended to complement other IGF community activities. Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics.

In the last three years, the BPF on Cybersecurity started investigating the concept of culture, norms and values in cybersecurity. In 2018 the BPF took a closer look at norms development mechanisms. In 2019, when the BPF ran in conjunction with the initiation of UN GGE and OEWG, the BPF looked at best practices related to the operationalization of cyber norms and started analyzing international and cross-stakeholder cybersecurity initiatives for commonalities.



BPF on Cybersecurity

- Culture, Norms and Values.
- Norms development mechanisms

BPF on Cybersecurity

- Identify Best Practices regarding norms operationalization
- Analyse international and cross-stakeholder agreements for commonalities

BPF on Cybersecurity

What can we learn from normative principles in global governance?

A working group investigated a variety of Cyber Norms initiatives and looked for strengths, weaknesses, and why they succeeded.

Exploring Best Practices in relation to international cybersecurity agreements

A working group identified new agreements, reviewed their relationship to the UNGGE 2015 consensus norms, and identified any new emerging norms.

What cybersecurity policymaking can learn from normative principles in global governance

The BPF 2020 took a wider approach and explored what can be learned from norms processes in global governance, in areas completely different than cybersecurity. Discussions during the BPF session at IGF 2019 in Berlin and the December 2019 informal intersessional consultative meeting of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, showed that the understanding of what is a norm and how norms work is not universal across the entire spectrum of norms and actors.

A working group within the BPF investigated a variety of different norms initiatives, to identify and define general characteristics of norms, how they arise and what they aim to change; to then take a deeper dive into their unifying effects: what works, what doesn't work, and how do they work.

The analysis identified several **factors that determine success in defining norms and their internalization**:

- Using the correct context and processes for norm construction in order to reach widespread acceptance.
- Employing strong leaders and resources for norm development.
- Ensuring the right elements of norm: identity, behavior, propriety, and expectation.
- Choosing the right tools of influence: incentives, persuasion, and socialization.

The analysis looked for common mistakes in norm-setting and identified a number of **risk factors inducing failure** of norm initiatives:

- Lack of clear outcomes.
- Lack of enforcement mechanisms.
- Too weak or too powerful leadership.
- Lack of incentives for internalizing norms.
- Domestic balance of power.
- Norms too specific or strict in wording.

To complete its framework, the team looked at how norms are promoted and enforced and documented a selection of existing enforcement mechanisms.

The case study analysis of successful norms frameworks, i.e. global nuclear norms, the Diplomatic Privilege and the Vienna Convention on Diplomatic Relations, the Sullivan Principles on Employment Practices, and the World Bank Guidelines in Treatment of Foreign Direct Investment, allowed to gather **lessons learned on process, content and implementation**.

- *On process*: Practically speaking the success in diplomatic norms are due to the excellence of the preparatory work and negotiating skills that led to the Vienna Convention.
- *On content*: The success of the global nuclear norms regime stems from its concreteness. In addition, the long stability of the basic rules of diplomatic law. Controversial issues such as diplomatic asylum were avoided and exceptioned. World Bank Guidelines on Treatment of Foreign Direct Investment are technically rigourous.
- *On implementation and enforcement*: The effectiveness of the Vienna Convention is also due to the norm of reciprocity as a sanction against non-compliance. While the Global Sullivan Principles perhaps only had widespread adoption and consensus because they lack concreteness, codification in binding documents and had few costs of violating those norms, they did give rise to more holistic frameworks for business ethics. The Global Sullivan Principles could be considered as a launching pad for more legitimate and enforceable processes in local contexts.

The research team summarized its **Lessons learned from norms initiatives in global governance** for the BPF session at the virtual IGF 2020 in three bullet points:

- Powerful norm promoters and ensuring incentives can be critical.
- Failures happen and are inevitable, but can become the basis for success.
- Norm development, even without results, creates socialization, which can be critical for further success.

Exploring Best Practices in Relation to International Cybersecurity Agreements

The 2020 BPF on Cybersecurity continued and further advanced the analysis of the 2019 BPF report on the state of international cybersecurity agreements, with a more narrow focus on cyber norms agreements.

Agreements were scoped into the analysis based on the following criteria:

- The agreement describes specific commitments or recommendations that apply to any or all signatory groups;
- The commitments or recommendations must have a stated goal to improve the overall state of cybersecurity; and,
- The agreement must be international in scope - it must have multiple well known actors that either operate significant parts of internet infrastructure, or are governments (representing a wide constituency).

Experts participating in the BPF identified 22 international agreements on cybersecurity norms for inclusion in this report, based on the scoping criteria above and split between three categories -- UN agreements, agreements within a stakeholder group, and agreements between multiple stakeholder groups. Each of the international cybersecurity agreements was reviewed based on i) when they were initiated, ii) which stakeholders are included, iii) the total number of supporters/signatories, iv) whether there is an organization responsible for maintaining the agreement, v) whether any of the eleven UN-GGE norms[1] are reflected in the agreement, and vi) what other norms are featured.

The decision to use the UN-GGE norms as basis for the analysis of other cybersecurity agreements is due to the unique responsibility the United Nations has in matters of international peace and security, and the recognition of the GGE’s 11 norms by consensus of the UN General Assembly. This was an effort to determine whether or not these multilateral cyber norms are being recognized and reinforced in other agreements in order to be strengthened, implemented, or enforced – including with non-state stakeholders.

The BPF’s analysis showed that the sixth norm, calling for cooperation to promote stability and security in cyberspace, was the norm most commonly reflected in the other agreements, with some form of it being evident in 77% of the agreements reviewed. It is perhaps unsurprising that the norm most commonly found in such agreements is that there should be partnership and cooperation between the parties in the agreement. The next most frequently recognized norm was number five, which is reflected in 68% of the agreements and recognizes either human rights or privacy rights online. States preventing

[1] Norms of Responsible State Behaviour in Cyberspace, as Agreed in the UN Group of Government Expert Reports of 2010, 2013 and 2015 https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

their own territory from being used in wrongful ICT acts, norm number one, was the UN norm least often reflected in other agreements.

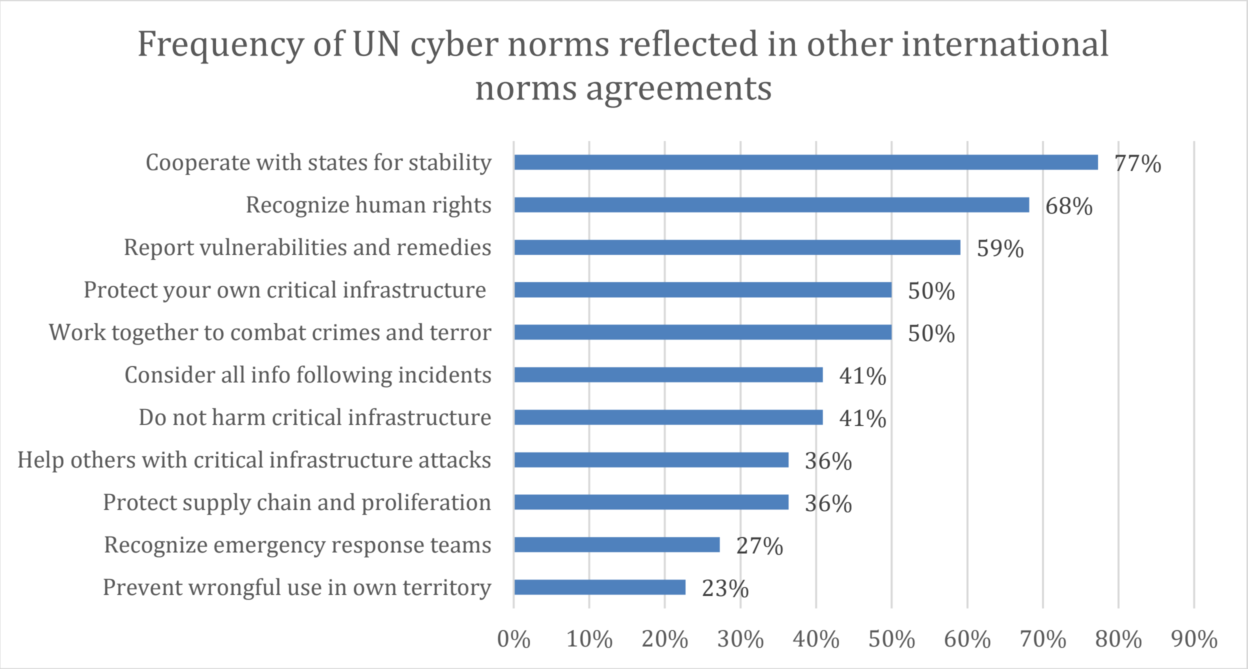


Table of Contents

PART I - What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance

The Internet Governance Forum's thematic intersessional work on cybersecurity intends to guide submissions to the 2020 Best Practice Forum on Cybersecurity's final, annual report. By taking the time to identify successful norms initiatives and their role in policy change, the BPF Cybersecurity grounds its analysis of a wide variety of Cyber Norms initiatives in the lessons learned throughout the stages from early development to implementation. The examples studied in this review were chosen for their effectiveness and are not necessarily related to or even tangential to technology or the Internet. By looking to successful norms frameworks the BPF Cybersecurity, and the initiatives it has invested in, might better understand the strengths, flaws, and why some norms initiatives have ultimately succeeded.

Editor: Mallory Knodel,
Authors: Apratim Vidyarthi, Anastasiya Kazakova,
Contributors: Maarten Van Horenbeeck, Sheetal Kumar,
Copy: Wim Degezelle.

Table of Contents

Introduction

The *Internet Governance Forum (IGF)* is a global forum convened by the United Nations Secretary General[2] where governments, civil society, the technical community, academia, the private sector, and independent experts discuss Internet governance and policy issues.[3]

The IGF *Best Practice Forums (BPF)* provide platforms for experts and stakeholders to exchange and discuss best practices in addressing Internet policy issues in a collaborative, bottom-up manner. BPFs intend to contribute to an understanding of global good practice, inform policy discussions, standards development, business decisions, as well as public understanding, awareness, and discourse.

In 2018 the BPF on Cybersecurity started work on "culture, norms and values" in cybersecurity. Its final report that year established the value of normative behavior in cyberspace, and identified the spaces in which norms can be developed. We adopted Katzenstein's definition of norms as a "collective expectation for the proper behavior of actors with a given identity", and noted how "the development of norms requires a shared belief about proper behavior for actors (in political science, usually states) in a community." The BPF determined that norms development in cyberspace however, was happening in many different spaces, some multilaterally between states, but also some in which a much wider set of participants took part, including civil society and the technical community. Examples of normative work identified include both policy norms, for instance "do not attack the public core of the internet," as well as purely technical elements, such as "implement a specific best practice" to reduce DDoS attacks.

Then in 2019 the BPF subsequently worked to identify a much larger set of documents published by a variety of actors, some implementing "hard law", and others putting forward "norms of behavior". For each of these, the BPF determined whether the documents reflected a core set of criteria, including the applicability of law on cyberspace and whether human rights were referenced.

Looking ahead to the 2020 intersessional report, members of the BPF reflected that little attention had been paid to the experiences of other areas in which norms have played a role in positive change. In particular during the Open-Ended Working Group[4] on developments in the field of information and telecommunications in the context of international security, and during the BPF session at the 2019 Internet Governance Forum in Berlin, several academics shared perspectives that went beyond those

[2] G.A. Res. 70/125 at 1 (Feb. 1, 2016) (extending the mandate of the IGF as set out in paragraphs 72 to 78 of the Tunis Agenda).
[3] The IGF is one of the key outcomes of the World Summit for the Information Society (WSIS). INTERNET GOVERNANCE FORUM, https://www.intgovforum.org/multilingual/ (last visited Dec. 11, 2020).
[4] Open-Ended Working Groups (OEWGs) report to the General Assembly, and provide the opportunity of holding "consultative meetings with industry, NGOs, and academia." *Open-Ended Working Group*, UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS, https://www.un.org/disarmament/open-ended-working-group/ (last visited Dec. 11, 2020).

often presented in cybersecurity. This paper takes a critical look at other areas, identifies learnings from norms development, and reviews how they can be applied to norm setting in cyberspace.

Why Norms Matter in Cyberspace

Norms are particularly well suited to cyberspace as a mechanism since the Internet is not developed, maintained, governed, or managed by any one stakeholder group; nor is it contained by national boundaries. This creates jurisdictional and policy-authority ambiguity. As a result, top down decision-making is rare, often limited in scope and impact, and thus ineffective. States and organizations can agree on bilateral decisions, but as protocols are typically global, and systems interoperate across the borders of these entities, universal agreements are needed but are not easily achieved.

The 2018 BPF also determined that Internet governance relies on multistakeholderism, making it even less likely that agreements are achieved between all parties nor encoded in written laws or contracts. This again makes the case for softer mechanisms in which agreement is developed over time, and results in pockets of agreement cascading into a more “widely accepted” norm.

Further, the BPF on Cybersecurity concluded in 2019 that different norm initiatives are filling gaps where more binding policy measures are not possible because of a lack of collective understanding of what the issues are and no agreement among stakeholders on adequate mitigations. However, there exist the beginnings of consensus expectations that, across different initiatives, can become a common basis to build on. Furthering these processes by focusing on identifying common goals and then fulfilling those goals with the requisite creativity is optimized by multistakeholder and multidisciplinary collaboration.

Analysing Cybersecurity Agreements

For norms codified in documents, which the 2019 BPF Cybersecurity report refers to as “cybersecurity agreements,” not every cybersecurity agreement analysed reflects a norm, since some agreements take on the perspective of being a “hard law,” in which non-compliance may be effectively addressed with enforcement activities.[5] Attention was paid to what degree specific agreements were of a binding nature. Cyber norms, in particular, are often nonbinding, but lead to reputational challenges, or other protest, when not adhered to.

Cybersecurity agreements were initially scoped in agreements based on three high level criteria:

[5] *Cybersecurity Agreements: Final BPF Output Report*, INTERNET GOVERNANCE FORUM (Jan. 2020), https://www.intgovforum.org/multilingual/filedepot_download/8395/1896.

- The agreement describes specific commitments or recommendations that apply to any or all signatory groups (typically governments, non-profit organization or private sector companies);
- The commitments or recommendations in the agreement have a stated goal to improve the overall state of cybersecurity;
- The agreement must be international in scope and include multiple well-known actors that either operate significant parts of Internet infrastructure, or are governments (representing a wide constituency).

The report determined that analysed agreements typically have four horizontal components:

1. Foundational principles, which guide development of norms or agreement. E.g. a commitment to accountability or cooperation, or to international law.
2. Definitions, which ensure a common understanding of terminology used in the agreement. In cybersecurity specifically, due to often very wide interpretation of terms, this is a critical component of achieving any level of agreement.
3. Implementation efforts, which are often not part of the agreement itself, but are initiatives launched on the sidelines to ensure the agreement is appropriately adhered to, socialized, or implemented.
4. Initiatives with broad support: initiatives that drive specific positive change, such as work on vulnerability disclosure or vulnerability equities processes.

After reviewing each agreement to identify whether specific, common elements were part of the discussion, the following key elements stood out:[6]

- Furthering multistakeholderism: identifying or supporting cybersecurity depends on the presence of all stakeholder groups in debate and coordination.
- Responsible disclosure: the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
- Referencing International Law: the agreement mentions the importance of international law, or commits the signatories' behavior to international law.
- Defining cyber threats: the agreement proposes a clear or aligned definition of cyber threats.
- Defining cyberattacks: the agreement proposes a clear or aligned definition of cyberattacks.
- Referencing capacity building: the agreement makes specific references to capacity building as a needed step to improve cybersecurity capability.
- Specifying confidence building measures (CBMs): the agreement describes or recommends specific CBMs.
- Referencing human rights: the agreement reflects on the importance of human rights online.
- Referencing content restrictions: the agreement discusses the need for content restrictions online.

[6] *Id*.

- Vulnerability equities processes: stockpiling of vulnerabilities may reduce overall cybersecurity, and so identifying processes that can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.

Placing Value in Norms Development

Not all established norm initiatives lead to policy changes. However, this does not indicate that these collective efforts are useless unimpactful. Norms are not static products, but socially dynamic processes, and their value is embraced in the processes themselves: continuously investing resources in the development of norms helps understand the most optimal way, given the particular context, to make norms work. This learning process includes recognizing possible blind spots, "closed doors," and insights and new factors that can facilitate norm development. Global governance regimes have put considerable time and effort into emerging as widely supported constructs, and engaging in defining and promoting norms requires patience as well.

The key lessons-learned in norms development could be briefly characterised as follows:

1. Certain critical factors matter.[7] while it is important to have influential powerful norm promoters, incentives for others to support norm development are not always sufficient, leading to failure. We also analyze what possible factors can enforce others' support of norm development, or, on the contrary, make them oppose this process.

2. Failures happen and are inevitable, but they can become the basis for success. Norms can develop and evolve through state practice, or significant global events can foster the norm development process. However, since "we are in the relative infancy of thinking about this issue"[8] and are yet to define rules of the game in cyberspace and draw lines,[9] states can easily alter their positions, opinions and attitudes if doing so serves their interests. This complicates norm development and may lead to frustration – or, vice versa, make norms emerge and work. The lesson is that it is necessary to consider this and be prepared: we cannot exactly predict or control the entire norm development process because there are many factors to consider, and such factors may be out of the norm developers' control. However, even failures teach and create opportunities for further successful efforts.

[7] Martha Finnemore & Duncan B. Hollis, Constructing Norms for Global Cybersecurity, 110 AM. J. INT'L. L. 425 (July 2016), https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf.

[8] Tim Starks, *The State Department's Weary Soldier in America's Cyber War*, FOREIGN POLICY (May 13, 2015), https://foreignpolicy.com/2015/05/13/the-state-departments-weary-soldier-in-americas-cyber-war-christopher-painter/ (quoting Chris Painter, a former U.S. diplomat).

[9] Further evidence of this is seen in the fact that many states are only at the very beginning of the process to develop regulations, laws, and processes for cyberspace.

3. Norm development, even without results, socializes and increases participants' awareness and knowledge, which can be critical for further success. Norm promotion can fail if the environment is not yet ready for norms: potential supporters may lack knowledge, capacity and maturity to contest norms. Therefore, it is important to consider norm development as a process crucial to preparing the environment to make it flourish. Socialization as a part of this process helps increase capacities and the maturity of processes in the environment. Socialization can also trigger significant policy changes enhancing security and stability in cyberspace – without necessarily leading to public contestation of norms. [10]

[10] For instance, capacity building efforts might trigger a state's willingness to create processes, laws for cybersecurity or to publish their opinion on application of international law to cyberspace.

Basic terms: Defining Norms and Their Role in Policy Changes

While the implementation and operationalisation of cyber norms remains a challenge for all actors, understanding how norms can be better adopted and operationalised benefits from an analysis of existing norm adoption that has led to behaviour change in other fields. By understanding the factors and contexts that lead to successful norm operationalisation in policy communities elsewhere, the cybersecurity community can learn and be guided by these best practices.

In order to reach those lessons, first we establish basic terminology around norms, followed in the next section by a basic framework for the purpose of analysing the specific examples chosen in this paper.

Defining Norms

In the infamous United States Supreme Court case *Jacobellis v. Ohio*, Justice Potter Stewart invented the Casablanca Test to identify pornography: "I know it when I see it."[11] Defining norms suffer from the same fluidity: identifying them is easy, but defining them is hard. Given this fluid nature, we can categorize norms into implicit norms, such as those that outline social contracts and basic international conduct; and explicit norms that are outlined in treaties, agreements, and other laws. This paper is concerned with the latter.

In international law, norms are defined as "specific but tacit standards of what is socially and individually acceptable," which encompasses both implicit and explicit norms. [12] Within this broad definition, norms should be concrete and specific.[13] In contrast to implicit norms, the strongest category of explicit norms are defined in international law through the principles of *jus cogens*, which center around norms that are accepted and recognized by nation states and from which "no derogation is permitted."[14] *Jus cogens* principles commonly apply to customary international law, treaty provisions, and general principles of norms.[15] *Jus cogens* requires evidence – such as public statements, legal opinions, laws, and legal decisions – showing that these norms have been accepted and recognized,[16] and that a large majority of

[11] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

[12] Geoffrey Vickers, Values, Norms, and Policies, 4 POL'Y SCIENCES 103, 103 (1973).

[13] *Id*. at 104.

[14] International Law Commission, *Report on the work of the seventy-first session chapter V: Peremptory norms of general international law (*jus cogens*),* ⁋56, Part One, Conclusion 2, U.N. Doc. A/74/10 (2019) (https://legal.un.org/ilc/reports/2019/english/chp5.pdf).

[15] *Id*. at ⁋56, Part One, Conclusion 5.

[16] *Id*. at 56, Part One, Conclusion 6.

states accept these norms.[17] Under *jus cogens*, some norms form the bedrock of international law and are "so fundamental as to be nonderogable under any circumstances."[18] Examples include prohibitions on torture and genocide: while countries do commit such acts, they do not contend the existence of a legal authority to do so.[19] Such fundamental norms require consensus, widespread agreement of the peremptory nature of the norms, and the existence of international treaties or tribunals to criminalize the violation of these norms.[20]

This basic overview of international law reveals the existence of a hierarchy of explicit norms.[21] Yet norms in all tiers have some necessary requirements, though they may not be sufficient for each tier:

1. Concreteness or specificity through clarifying identity (whom to govern?), behavior (what does the norm say?), propriety (what is a basis for a sense of "oughtness"?), and expectations (is there consensus or collectively shared expectations for widespread acceptance?);
2. Framing contexts and creating right processes;
3. Powerful leadership and strong norm entrepreneurs; and
4. Tools of influence for norm promotion through creating incentives, using persuasion or applying socialization.

Sources of Norms

International law consists of bilateral and multilateral treaties, both of which reflect norms that are either being codified, or have already been translated into law and are being implemented.[22] This reflects a normative life cycle: first, norms emerge through social processes, often propagated by politically engaged entities.[23] Second, the norm is adopted, normally through transnational organizations socializing these norms.[24] Finally, the most difficult step is spreading the norm and garnering widespread acceptance using interactions between states and non-state actors, reflected in the internalization of the norm and its compliance.[25] Within this life cycle, non-governmental actors, intergovernmental actors, and states all play major roles in norm creation and acceptance.

While in some cases states are the final actor in the spread of a norm, the creation of the norm often happens outside the purview of state actors and the codification process. The codification process

[17] Jules Lobel, *Fundamental Norms, International Law, and the Extraterritorial Constitution*, 36 YALE J. INT'L LAW 307, 310 (2011) (https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1401&context=yjil)
[18] *Id*. at 308.
[19] *Id*. at 335.
[20] *Id*. at 340, 342.
[21] *Id*. at 339.
[22] Knut Traisbach, *International Law*, E-INTERNATIONAL RELATIONS (Jan. 1, 2017), (https://www.e-ir.info/2017/01/01/international-law/).
[23] *Id.*
[24] *Id.*
[25] *Id.*

transforms a conventional norm, such as an opposition to torture, into one of customary international law, such as the United Nations Convention Against Torture. States do this if the practice or norm is being followed out of a sense of legal obligation, or *opinio juris*.[26] Thus, to get from acceptable norms to fundamental or *jus cogens* norms requires legal obligation in practice. In cyberspace, we generally observe norm promotion and enforcement by certain states through public statements condemning norm violators – without clear references to particular treaties or laws that create legal obligation to follow the norm.[27]

Sources for norm-setting and norm development could be grouped into three categories, depending on the source of the norm:

- **Multilateral norm diplomacy and state-driven efforts:**
    - Joint statements: e.g. advancing responsible state behaviour;[28] tackling the "Infodemic."[29]
    - Joint proposals: e.g. malicious cyber activity against healthcare services.[30]
    - Exchange of views between states, either directly or at the premises of intergovernmental organizations.
    - Publications by states of their understanding and best practices: e.g. Australian implementation of norms of responsible state behavior in cyberspace.[31]
    - State-led and state-initiated processes with the participation of non-state actors: e.g. dialogues generally,[32] Global Commission on the Security of Cyberspace,[33] Paris Call for Trust and Security in Cyberspace[34].

[26] Ruzbeh B. Baker, *Customary International Law in the 21st Century: Old Challenges and New Debates*, 21 EUROPEAN J. INT'L LAW 173, 173 (2010) (https://academic.oup.com/ejil/article/21/1/173/363352)

[27] Recent examples include public statements of states (Canada, the U.K. the U.S. and other NATO countries) condemning Russia's malicious cyber-activity targeting Georgia (2020) or statements of the EU representatives and the U.K condemning China's malicious cyber-activity. *See, e.g.* CSE Statement on Malicious Russian Cyber Activity Targeting Georgia, COMMUNICATIONS SECURITY ESTABLISHMENT OF CANADA (Feb. 21, 2020), https://cse-cst.gc.ca/en/media/2020-02-21.

[28] *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, U.S. DEPARTMENT OF STATE (Sep. 23, 2019), https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

[29] *Cross-Regional Statement on "Infodemic" in the Context of COVID-19*, PERMANENT MISSION OF AUSTRALIA TO THE UNITED NATIONS, https://unny.mission.gov.au/files/unny/120620%20Cross-Regional%20Statement%20on%20Infodemic%20in%20the%20Context%20of%20COVID-19.pdf (last visited Dec. 11, 2020).

[30] *Malicious Cyber Activity Against Healthcare Services and Facilities: Joint OEWG Report*, UNITED NATIONS, https://front.un-arm.org/wp-content/uploads/2020/05/final-joint-oewg-proposal-protection-of-health-infrastructure.pdf (last visited Dec. 11, 2020).

[31] *Australian Implementation of Norms of Responsible State Behaviour in Cyberspace*, AUSTRALIAN GOVERNMENT DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf (last visited Dec. 11, 2020).

[32] *See, e.g. Geneva Dialogue on Responsible Behavior in Cyberspace*, GENEVA DIALOGUE (Last accessed Dec. 11, 2020), https://genevadialogue.ch/.

[33] GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE, https://cyberstability.org/ (last visited Dec. 11, 2020).

[34] PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE, https://pariscall.international/en/ (last visited Dec. 11, 2020).

    - Public consultations organized by states for non-state actors to share their understanding of norms and ways to operationalize it: e.g. Australian public consultation.[35]
    - Publishing compilations of norm implementation guidance: e.g. Australian compilation.[36]

- **Subject-matter, expert-driven and civil society efforts:**
    - Analyzing norm definition and norm operationalization: e.g. The Hague Program for Cyber Norms,[37] Global Partners Digital's work on analysing norms.[38]
    - Establishing calls to governments to agree on certain norms of behavior: e.g. The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector,[39] ICRC's call to global leaders to stop cyberattacks on healthcare sector.[40]

- **Industry-led processes:**
    - Establishing calls to governments to agree on certain norms of behavior: e.g. Digital Geneva Convention,[41] Manifesto for a New Digital Deal.[42]
    - Establishing industry organizations based on participants' consensus around particular norms of behavior: e.g. Charter of Trust,[43] Tech Accord.[44]
    - Establishing initiatives for norm operationalization, including developing of confidence building and capacity building efforts: e.g. Global Transparency Initiative.[45]

[35] *Public consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations*, Australian Government Department of Foreign Affairs and Trade, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/public-consultation-responsible-state-behaviour-in-cyberspace-in-the-context-of-international-security-at-the-united-nation (last visited Dec. 11, 2020).

[36] *Summary Of Public Submissions On Developing Best Practice Guidance On Implementation Of The 11 Norms Of Responsible State Behaviour In Cyberspace Articulated In The 2015 GGE Report (A/70/174), As Endorsed By The UN General Assembly (A/RES/70/237)*, Australian Government Department of Foreign Affairs and Trade (June 2020), https://www.dfat.gov.au/sites/default/files/compilation-norm-implementation-guidance.pdf.

[37] The Hague Program for Cyber Norms, https://www.thehaguecybernorms.nl/ (last visited Dec. 11, 2020).

[38] Anriette Esterhuysen, Deborah Brown & Sheetal Kumar, *Unpacking The GGE's Framework On Responsible State Behaviour: Cyber Norms*, Global Partners Digital (Dec. 19, 2019), https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/.

[39] *The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*, Oxford Institute for Ethics, Law and Armed Conflict, https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea (last visited Dec. 11, 2020).

[40] *Call By Global Leaders: Work Together Now To Stop Cyberattacks On The Healthcare Sector*, Humanitarian Law & Policy (May 26, 2020) https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/.

[41] Brad Smith, *The Need for a Digital Geneva Convention*, Microsoft (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[42] A Manifesto for a New Digital Deal, Telefonica, https://www.telefonica.com/digital-manifesto/ (last visited Dec. 11, 2020).

[43] Charter of Trust, https://www.charteroftrust.com/ (last visited Dec. 11, 2020).

[44] Cybersecurity Tech Accord, https://cybertechaccord.org/accord/ (last visited Dec. 11, 2020).

[45] Kaspersky Global Transparency Initiative, Kaspersky, https://www.kaspersky.com/transparency-center (last visited Dec. 11, 2020).

Types of Policy Change

Policies themselves can be defined strictly as a series of regulatory or legal rules (formal change), or more broadly as studies written by the government, assessments, and visions (intents to change). Policy changes can be categorized based on subject matter, actor, time span, method, and a variety of other factors. Within the notion of norm development or change, it makes most sense to look at policy change based on how actors interact: either unilaterally, or multilaterally through treaties, international organizations, or frameworks and conventions.

Unilateral policy change, such as de-escalation or denuclearization, allows states to virtue signal, especially if the state is a global leader that shapes policy. Given that unilateral policy changes are domestic or internal changes, they consist of de jure change (how the policy is written) and de facto change (how the policy is implemented). Unilateral policy changes – especially in the context of the Internet – are less relevant to norm implementation, given that norms require widespread acceptance and multistate codification and signature.[46]

Multilateral policy changes are effectuated through agreements between multiple states, or through international actors. With the latter, states often play a significant role, though some international actors, such as the IETF, do not necessarily require states to play major roles. Non-state actors and states alike are involved in international organizations, which implement legal arbitration, dispute resolution, preventative policies, and norm setting; and in frameworks and conventions which implement soft law.[47] In this context, non-state actors play a role in the first part of the norm life cycle: formulating social processes or elevating them to the attention of international organizations. International organizations play the critical role of socializing these norms – the second step of the normative life cycle – by fleshing out the concrete details of these norms and advocating these norms to member entities or states. These organizations also formulate implementation mechanisms, including penalties, for violating these norms; however, such mechanisms and sanctions normally require state buy-in if the international organization itself is not able to execute these mechanisms and sanctions. States and international organizations play a part in the final step of the normative life cycle; states internalize the norms, while international organizations gather widespread acceptance. Unlike with international organizations, frameworks and conventions generally focus on the third step of codifying and gathering widespread acceptance of norms, and play a role when norms are already well-known and have some acceptance.

[46] *See supra* Defining Norms at 8.

[47] Kenneth W. Abbot and Duncan Snidal, *Hard and Soft Law in International Governance*, 52 INT'L ORG 421, 434 (2000), http://www.jstor.com/stable/2601340.

Framework and Analysis: Getting Norms Right in Development and Implementation

Now that we have defined the characteristics of norms, how they arise and what they aim to change, we look into their unifying effects: what works, what doesn't work, and how these norms work.

What Makes Norms Development and Implementation Successful?

There are several factors that determine success in defining norms and their internalization:

- **Understanding contexts and creating the correct processes for norm construction and reaching widespread acceptance**: treating norms not as abstractions or products, but perceiving them as 'social creatures' that emerge out of specific contexts and are supported by certain social processes and interactions among groups of actors.[48] The success of a norm does not depend much on what the norm says, but who accepts the norm, where, under which conditions, and how they do it – thus analyzing and creating correct processes, and choosing and framing the context for norm development seems essential. Framing the context for defining norms is not always easy to do and requires significant effort. Interested parties who promote norms (norm entrepreneurs) should first identify a problem or problems which a norm aims to solve. Then, once a correct context is selected (venue, platform, organization, level for addressing the problem: regional or global, etc.), it is possible to identify potential actors or participants in the process. Problems that norms aim to solve should also be linked to larger issues to be easily understood by wide groups of people and thus to attract potential supporters and resources. For example, framing a norm with states or organizations that suffered from cyberattacks might have a stronger effect in persuading the broader community to accept the norm: open and public support to the norm from the victims of cyberattacks creates additional legitimacy in norm promotion.

- **Having powerful leaders as norm entrepreneurs and allocating sufficient resources for norm development:** norm entrepreneurs are key interested parties or actors during the first stage when a norm emerges. Norm entrepreneurs can be individuals (e.g. Henry Dunant, founder of the International Committee of the Red Cross), states, non-governmental organizations (e.g. Amnesty International), private sector entities (e.g. Microsoft), or international organizations (e.g. the UN). Powerful, influential and widely respected leaders and/or a 'high-ambition coalition' of states can be crucial for norm emergence and for encouraging others to give

[48] *See* Finnemore & Hollis, *supra* note 6.

support. [49] It might be also easier to develop shared expectations in a smaller group concerned by the same problem (e.g. 2015 US-China bilateral agreement on cyber-espionage for commercial advantage). Norm entrepreneurs having sufficient resources, ambition and persistence therefore may define success in norm promotion.

- **Ensuring all four elements of norms: identity, behavior, propriety, and expectation.**
    - Identity: To identify a norm when we see one, it is important to link specific actors to desirable behavior and therefore answer the question 'whom does the norm govern?'
    - Behaviour: Norms are created to address particular problems and should be specific in communicating specific actions that need to be taken (*behaviour*) – 'what does the norm say?'
    - Propriety: To influence norm promotion, it is important to provide a basis on which norms shape expectations and create a sense of 'oughtness' (*propriety*). These could be treaties, political commitments, customary international law, domestic law, and/or cultural and professional norms.
    - Expectations: Norms fail without collectively shared *expectations* in a community about a particular prescribed behavior – through collective efforts it would only be possible to define and promote norms as a social construction widely understood and shared.

- **Choosing and leveraging tools of influence: incentives, persuasion, and socialization:** norms are not static products, but are dynamic ongoing processes of social constructions that evolve depending on the right context. It is in the power of norm entrepreneurs to employ tools of influence, which fall into three categories – incentives, persuasion, and socialization – and it is up to norm entrepreneurs to maneuver and decide which tool fits the context better.
    - Incentives should be aligned with state behavior. Without these incentives, states would not be motivated to adopt norms. Incentives are applied when norm entrepreneurs create political attractiveness and value for specific actors – for instance, through international legitimation for these actors or through creating value for domestic legitimacy. International organizations as norm entrepreneurs can be particularly attractive for other actors as 'custodians of the seals of international approval and disapproval,'[50] and, particularly, conformity to norms can be ensured if actors get opportunities to avoid disapproval as a result of norm violation happened in the past. However, using incentives is effective when they are actively used for a long period of time; otherwise, if norm entrepreneurs stop putting efforts into maintaining the incentives, adherence of supporters might end.

[49] Christian Ruhl, Duncan Hollis, Wyatt Hoffman & Time Maurer, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Proesses at a Crossroads*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Feb. 2020), https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf.

[50] Inis L. Claude, Jr., *Collective Legitimization as a Political Function of the United Nations*, 20 INT'L ORG. 367 (1966), https://www.jstor.org/stable/2705629.

- Persuasion can be coupled with incentives, and should be clearly targeted – approaching actors with different value systems could be problematic. What can be effective for one group of actors – e.g., civil society community, would hardly be relevant (as a message) to cybercriminals to change their behavior and adhere to the norm.
- Socialization implies efforts to teach particular groups (the smaller and more homogenous, the better) about the norm and thus impact norm compliance through creating common language and a common network. Capacity building, building communication networks and communities, providing technical assistance, training and learning courses are examples of socialization as a tool of influence.

What Are Anti-Patterns in Norm-Setting?

In analyzing factors that either facilitate or prevent norm-setting, it is necessary to look at norms not as static products but as dynamic processes, i.e., social constructions that are shaped by the contexts and interactions of actors. Therefore, a search for common mistakes in norm-setting should be focused on analyzing the pace and directions of changes that happen in the norm context (environment). From that, we know that shared beliefs might change and new problems might arise, and therefore, contexts and group memberships might change too. **Lack of powerful leadership** and **lack of clearly assigned roles** in maintaining those shared beliefs as well as keeping them relevant for norm supporters are traps leading to failure in norm promotion.

Lack of clearly assigned roles among norm promoters, in particular, might lead to a **lack of clear outcomes** that norm-setting as a process generates to remain inherently dynamic.[51] Multistakeholder engagements for norm development make actors identify themselves with different groups and fulfil multiple roles. And if norms as a process do not stay dynamic and do not manifest particular outcomes, the risk of failure increases. However, besides a lack of clearly assigned roles and lack of dynamism to achieve outcomes, multistakeholder engagements comprised of actors with backgrounds, values, interests and incentives that are too different might also make negotiations more complicated in trying to achieve particular results, and make stakeholders less open to candidly discuss issues. [52] This is the second trap leading to failure. Thus, starting with a small group of actors that share the same values even though they represent different stakeholder groups would help engender norm-conformity.

However, though roles can be clearly assigned, those who promote norms might **lack mechanisms to enforce conformity or adherence to the norms**. This particularly applies to international bodies that often press norms without leverage other than modeling and light persuasion.[53] The absence of a

[51] *See* Finnemore & Hollis, *supra* note 6.

[52] Interests could be indeed different, but still overlap and support each other.

[53] Terence C. Halliday & Bruce G. Carruthers*, The Recursivity of Law: Global Norm Making and National Lawmaking in the Globalization of Corporate Insolvency Regimes*, 112 AM. J. SOCIO. 1135, 1170 (Jan. 2007).

centralized enforcement authority[54] with powers prevents from creating conditionalities that could be useful in implementing norms.[55] Conditionalities are an act of persuasion and therefore a tool of influence that creates attractiveness for actors to support norms. It should also be stated that conditionality can have limited success and be less effective than other tools, and to be successful, should be complemented with incentives, i.e., the promised reward needs to be greater than the cost of fulfilling the conditions of the reward.

The **lack of incentives for internalizing norms**[56] is another trap leading to failure in norm-setting. The prospective benefits of norm compliance should outweigh the prospective benefits of staying away from norm adherence or the promotion process. Possible incentives might be: domestic demand and attractiveness of norm compliance to enhance domestic legitimacy; international legitimation and acceptance; and esteem needs: actors "follow norms because they want others to think well of them, and they want to think well of themselves."[57]

Powerful leadership may not only positively impact norm-setting and sometimes even be a crucial factor in defining a norm, but may also break norms if it is in the interest of powerful leaders and if benefits outweigh the cost of not adhering to norms. This is particularly common in cases where there is a lack of enforcement powers, or where norm violation would not trigger significant consequences for 'norm breakers'. It should also be stated that norm-breaking behavior can also reveal alternative norms that the 'norm breaker' is more willing to promote – for instance, State A breaks a certain norm as it contradicts its domestic laws or norms, but in seeking international legitimation, State A does not simply start following the norm but starts framing new norms and new contexts, with or without providing 'propriety' (the basis for norms – treaties, customary international law or domestic law). When non-compliance leads to a cascade of norm violations, then violations become the rule rather than the exception.[58]

We mentioned earlier that the absence of some elements in norms (identity, behavior, propriety, and expectation) makes norms less specific and therefore makes it harder for norm entrepreneurs to garner attention, support and resources. However, at the same time, imprecise norms that have few specifics in wording might also provide more room for maneuver to attract actors with different backgrounds and therefore be less vulnerable to environmental changes as well as be more flexible and adaptive to those changes. Precise norms, on the contrary, might not be of much help in facilitating incremental change and might degenerate quickly.[59] Therefore, norms that are **too specific and strict in wording** might contain another common mistake leading to failure.

[54] Diana Panke & Ulrich Petersohn, *Why International Norms Disappear Sometimes*, 18 EUR. J. INT. RELATIONS 719, 732 (2012), https://www.researchgate.net/publication/258135219.

[55] Halliday & Carruthers at 1174.

[56] *See* Ruhl et al., *supra* note 48.

[57] Robert Axelrod, *An Evolutionary Approach to Norms*, 80 AM. POL. SCI. REV. 1095, 1105 (1986).

[58] Panke & Petersohn at 730.

[59] *Id*. at 732.

Domestic legal institutions and domestic powers can also play a critical role in a state's non-compliance with a norm. The actual decision of whether or not to adhere to or violate a norm often depends on or is made by domestic institutions. And when states break the norm or decide to stay out of the norm development process, this might indicate certain trade-offs; in particular, that reputational implications and possible sanctions for norm violation do not outweigh the interests of domestic powers (if these powers do not support norm adherence).[60] Thus, for norm entrepreneurs it can be useful to consider the domestic balance of power within a particular state to create the appropriate processes and frame the norm so that the norm as a process would be aligned (as much as is possible) with the state's domestic laws or powers.

How Are Norms Enforced?

In promoting or enforcing norm adherence, the following are a selection of enforcement mechanisms:

- **Supporting norm legalization and codification.** Some norms first appear as best practices, but over time can be legalized and become a part of law**.** Therefore, costs for non-compliance with norms increase as they become risks of non-compliance with regulatory measures. For instance, norm (j) in the 2015 GGE report[61] on responsible reporting of vulnerabilities – which also exists and is implemented in best practices such as FIRST's Code of Ethics[62] or Kaspersky's Ethical Principles for Responsible Vulnerability Disclosure[63] and recently appeared in the public consultation to review and update the EU NIS Directive (though vulnerability management and disclosure has not been a part of the NISD framework).[64]

- **Grafting new norms onto existing institutions.** This, in particular, allows the creation of legitimacy and the reduction of effort and startup costs for norm entrepreneurs, and thus makes the norm-setting process more attractive for them. As an example, the currently discussed dual-use export controls and derogations for vulnerability disclosure are part of the Wassenaar Arrangements, which are the successor to the Cold-War-era Coordinating Committee for Multilateral Export Controls (COCOM).

[60] *Id.* at 725.

[61] G.A. Res. A/70/174 at 8 (July 22, 2015).

[62] *Ethics for Incident Response and Security Teams*, FIRST, https://www.first.org/global/sigs/ethics/ethics-first (last accessed Dec. 12, 2020).

[63] *Kaspersky's ethical principles in Responsible Vulnerability Disclosure*, KASPERSKY, https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/05/15091233/RVD-Ethical-Principles-EN.pdf (last accessed Dec. 12, 2020).

[64] *Review of EU rules on the security of network and information systems*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems (last accessed Dec. 12, 2020).

- **Favoring fragmentation and cross-pollination of cyber norms efforts together with promoting multistakeholder engagements.** [65] Fragmentation can help address different actors and, if specifically focused on a relatively small group of stakeholders, norms can be even more efficient in changing behavior and creating new collectively shared expectations (norms for industry vs. norms for all states). The more initiatives addressing needs and interests appear, the more incentives and motivations are created for active participation of different stakeholders in norm development. Multistakeholder engagements can also provide more resources for further norm construction, even though actors might follow different goals in publicly adhering to the norm.

- **Creating network sanctions**.[66] These can be effective in not only making particular actors follow norms, but also in exerting pressure on actors to facilitate domestic reforms that would create a basis (propriety) for the actor to follow the norm further. If networks are important to actors, then those actors would rather decline the risk of possible network sanctions (that arise from norm violation) to avoid their relationships being impaired. And vice versa, if norm adherence may improve an actor's status among network peers and when it competes with domestic interests, the actor will still be willing to comply with a network norm.[67]

- **Applying diplomatic sanctions**. Most sanctions are targeted as they have the 'normative virtue of not punishing an entire population' for the actions of a small governing minority. [68] Sanctions might include arms embargoes, travel bans, freezing of assets, and economic restrictions (import or export bans on certain goods, investment bans, and technology bans, i.e., prohibitions on supplying certain services, technologies, etc.). The EU Cyber Diplomacy Toolbox, established in May 2019 as a cyber-sanctions regime, is a key example of these enforcement mechanisms for norm compliance in cyberspace. However, it is yet to be seen if these mechanisms are effective in practice: the adoption of sanctions usually imposes costs on both sides (the sanctioned and sanctioning states), and therefore to make the 'punishment' work, incentives should be provided to sanctioning states as well.

- **Targeting reputation and self-esteem of 'norm breakers'.** Reputational benefits as one of the incentives for norm compliance can be targeted for enforcing norm adherence. This may include public criticism, refusal of other states to enter into future agreements with a 'norm-breaker' or keeping current agreements, and/or withdrawal of membership from international organizations and closed groups or clubs.

[65] *See* Ruhl et al., *supra* note 48.
[66] Charles K. Whitehead, *What's Your Sign? - International Norms, Signals, and Compliance*, 27 Mich. J. Int. Law 717, 717 (2006) (https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1204&context=mjil)
[67] *Id*. at 719.
[68] *Guardian of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace*, 155 EUROPEAN UNION INST. FOR SECURITY STUD. 12 (Oct. 2019), https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf.

Case Studies: Analyzing Successful Global Norms

Using the norms test defined in Section II, we analyze a variety of successful frameworks to understand their strengths, flaws, and why they ultimately succeeded. The test has four parts: (1) concreteness or specificity; (2) consensus or widespread acceptance; (3) norms codification in legal documents that are signed by countries forming the consensus; and (4) costs of violating those norms.

Global Nuclear Norms

The global nuclear industry consists of nuclear energy for peaceful purposes (such as research, energy, medicine, and space exploration) and for armed conflicts (such as nuclear weapons). Since the mid-1960's, global nuclear norms have focused on nuclear restraint, encompassing deterrence, non-use, and nonproliferation.[69] These norms cover the end-to-end nuclear supply chain, from the mining of nuclear materials, to the disposal of nuclear waste.

The success of the global nuclear norms regime stems from its concreteness. Nuclear norms have been codified in the Nonproliferation Treaty (NPT), where signatories agree to give up or never acquire nuclear weapons, in exchange for access to peaceful nuclear technology.[70] The NPT is supplemented by bilateral treaties between major nuclear powers (e.g. the U.S.-Russia Strategic Arms Limitation Treaty of the 80's), test ban treaties (e.g. the Comprehensive Nuclear Test Ban Treaty). The NPT is also supported by technical treaties that delineate protocols regarding the specifics of nuclear energy, such as the Convention on Nuclear Safety and the Convention on the Physical Protection of Nuclear Material. These treaties or frameworks have specific, scientific details around what kinds of nuclear materials can be acquired, how monitoring and enforcement takes place, and technologies that can be used. The specificity arises from the involvement of experts in the drafting and enforcement processes.

In addition to the concreteness, non-proliferation is widely accepted. The NPT has been signed by 191 UN members, making it the most ratified arms limitation/disarmament treaty.[71] The widespread acceptance of nonproliferation as a goal, combined with its codification and ratification, has largely internalized nonproliferation as a bedrock of international relations. Note that this widespread acceptance was not organic, but propagated by major nuclear powers, combined with the cultural fear of nuclear weapons and nuclear war. The costs of violating these nuclear norms, including sanctions and an embargo on access to nuclear technologies, has forced the continued existence of these norms,

[69] Lawrence Freedman, *Disarmament and Other Nuclear Norms*, 36 WASH. Q. 92, 108 (2013).
[70] Treaty on the Non-Proliferation of Nuclear Weapons Preamble, May 11 1995, 21 U.S.T 483, 729 U.N.T.S. 161.
[71] Treaty on the Non-Proliferation of Nuclear Weapons (NPT), United Nations, https://www.un.org/disarmament/wmd/nuclear/npt/ (last visited July 1, 2020).

leading to only one country leaving the NPT - North Korea - and thereby facing massive economic turmoil and becoming a political outcast. Finally, combined with widely accepted nuclear norms infrastructure, like the Nuclear Suppliers Group (NSG) cartel that has a monopoly on nuclear materials, the original widespread acceptance is forced onto countries, which have to comply in order to get access to nuclear materials.

Despite its successes, global nuclear norms have faced some challenges. Regulations are extremely expensive and cumbersome, stifling the innovation of new nuclear reactors. The goal of nonproliferation, combined with the risks of proliferation, have created a culture of risk-averse actors and government regulators in countries like the U.S., and thus a negative public image of the industry. Finally, political disputes often begin to encompass nuclear issues, preventing norm enforcement and prolonging disputes, such as in the India-Pakistan region.

Diplomatic Privilege and The Vienna Convention on Diplomatic Relations

The Vienna Convention on Diplomatic Relations has codified the custom of diplomatic immunity, which has been present for millennia.[72] The Vienna Convention allows for the granting of certain privileges and immunities to diplomats, which allows for diplomats to carry out their duties.[73] Home countries have the right to waive diplomatic immunity, though this happens rarely.

The Vienna Convention reflects the norm cycle and how widely accepted social customs have been adopted by international actors and eventually codified into international law. Its success are due not only to the excellence of the preparatory work by the International Law Commission and the negotiating skills of State representatives at the Conference, but also to the long stability of the basic rules of diplomatic law and to the effectiveness of reciprocity as a sanction against non-compliance:

> “The success of the Conference and of the Convention which it drew up may be ascribed first to the fact that the central rules regulating diplomatic relations had been stable for over 200 years. Although the methods of setting up embassies and communicating with them had radically changed, their basic functions of representing the sending State and protecting its interests and those of its nationals, negotiation with the receiving State, observing and reporting on conditions and developments there remained and still remain unaltered. Secondly, because the establishment of diplomatic relations and of permanent missions takes place by mutual consent, every State is both a sending and receiving State. Its own representatives abroad are in a sense hostages who may on a basis of reciprocity suffer if it violates the rules of diplomatic immunity, or may be

[72] Jovan Kurbalija, Dietrich Kappeler & Christiaan Sys, *Evolution of Diplomatic Privileges and Immunities,* DIPLOMACY.EDU (2008), https://www.diplomacy.edu/resources/general/evolution-diplomatic-privileges-and-immunities.
[73] Vienna Convention on Diplomatic Relations art. 31, 1961, S. Treaty Doc. No. 92-12 , 500 U.N.T.S. 95.

> penalized even for minor restrictions regarding privileges or protocol. There was at the 1961 Vienna Conference no general underlying conflict of interest between opposing groups of States."[74]

The successes of the Vienna Convention can be ascribed to the initial narrowness of the principles, followed by the eventual acceptance and expansion of those principles as nations began to accept the norms broadly:

> "Avoiding controversial issues such as diplomatic asylum and focusing on permanent envoys rather than on ad hoc representatives or other internationally protected persons, the convention accorded immunity from criminal prosecution and from some civil jurisdiction to diplomats and their families and lesser levels of protection to staff members, who generally were given immunity only for acts committed in the course of their official duties. Since the 19th century, diplomatic privileges and immunities have gradually been extended to the representatives and personnel of international organizations."[75]

Effectively, the Vienna Convention fulfills all four requirements: concreteness, widespread acceptance, codification in international law, and penalties for failure to adhere to these norms.

The Sullivan Principles on Employment Practices

The Sullivan Principles were a code of conduct that called for desegregation in the workplace, equal pay, and equal employment practices, and was signed by U.S. companies during the Apartheid era.[76] These principles led to the development of Global Sullivan Principles (GSP), which advance human rights and social justice internationally.[77] The principles affected the welfare of workers and the work environment, despite not being a treaty and being signed on voluntarily by companies like Nike, Gap, and Levi Strauss.[78] While the original Sullivan Principles have mixed reviews and were considered as not going far enough,[79] many companies signed on to the principles, and these companies did better on the stock

[74] Eileen Denza, *Vienna Convention on Diplomatic Relations: Introductory Note*, AUDIOVISUAL LIBRARY OF INTERNATIONAL LAW, https://legal.un.org/avl/ha/vcdr/vcdr.html (last accessed Dec. 12, 2020).

[75] *Diplomatic Immunity*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/diplomatic-immunity (last accessed Dec. 12, 2020).

[76] Steven R. Ratner, *International Law: The Trials of Global Norms*, 110 FOREIGN POLICY 65, 72 (1998) (http://www.jstor.com/stable/1149277).

[77] The Global Sullivan Principles, UNIVERSITY OF MINNESOTA HUMAN RIGHTS LIBRARY, http://hrlibrary.umn.edu/links/sullivanprinciples.html (last accessed July 1, 2020).

[78] Ratner at 72.

[79] Corporate Response: The Sullivan Principles, MICHIGAN IN THE WORLD AT THE UNIVERSITY OF MICHIGAN, https://michiganintheworld.history.lsa.umich.edu/antiapartheid/exhibits/show/exhibit/origins/sullivan-principles (last accessed July 1, 2020).

market than stock averages.[80] Additionally, the original Sullivan Principles encouraged companies to withdraw from South Africa when the principles were violated or unimplementable.[81]

Within the four factors for norms, the newer GSP (coming into effect in 1999) lack specificity or metrics against which to measure accomplishment.[82] They are also not widely accepted, given that it is an opt-in framework that pertains to private companies and multinationals, and not nation states. And there are minimal explicit costs to failing to sign on or violating the GSPs - given the lack of enforcement mechanisms, outside of the opportunity cost of signing on to them and receiving positive recognition for doing so.[83] Nonetheless, the norms have been codified in the GSP, which companies can sign, and then are invited to an annual meeting and required to submit a report posted to the GSP website.[84] Given that the norms fulfill one out of the four factors, they may be evaluated as less successful than the other case studies in this paper. However, the GSP did give rise to more holistic frameworks for business ethics, including the United Nations Global Compact with Business.[85] In a sense, the GSP could be considered as a launching pad for creating a more legitimate, enforceable normative framework.

World Bank Guidelines on Treatment of Foreign Direct Investment

While the World Bank's Guidelines are not binding on any bank member, these guidelines are considered the standard for how developing nations should treat foreign capital for encouraging investment.[86] These Guidelines are a soft law that acts as a standard for global regulations.[87] The guidelines are not binding, but influence new laws and treaties by promoting the movement of capital internationally.[88] They are also a model for national laws.[89]

Applying the test for norms, we see that these guidelines have specific details that provide information about Foreign Direct Investment parameters and processes; and that these have been codified and are somewhat widespread. However, these guidelines are entirely optional, not signed by countries, and are not associated with enforcement mechanisms. Nonetheless, the optional nature creates an environment where these guidelines have become widespread, given the association with the World Bank and the technical correctness of the guidelines.[90]

[80] Malek K. Lashgari & David R. Grant, *Social Investing: The Sullivan Principles*, 47 REV. SOCIAL ECON. 74, 80 (1989).

[81] Mzamo P. Mangaliso, *South Africa: Corporate Social Responsibility and the Sullivan Principles*, 28 J. BLACK STUD. 219, 229 (1997).

[82] Gwendolyn Yvonne Alexis, GREEN BUSINESS: AN A-TO-Z GUIDE (Nevin Cohen Ed., 2010).

[83] Geral F. Cavanagh, *Global Business Ethics: Regulation, Code, or Self-Restraint*, 14 BUS. ETHICS Q. 652, 638 (2004).

[84] *Id.* at 633.

[85] *Id*.

[86] Ratner, *supra* note 73 at 68.

[87] *Id*.

[88] Ardeshir Atai, *Comparative Analysis of the Iranian Foreign Direct Investment Law and the World Bank Guidelines on Treatment of Foreign Direct Investment*, 12 YEARBOOK OF ISLAMIC AND MIDDLE EASTERN L. ONLINE 111, 113 (2005).

[89] *Id*.

[90] *Id.*

Conclusions: Lessons for Cybersecurity Policymakers on Norms

The BPF on Cybersecurity in 2019 launched and worked during important events for the international community when two parallel processes - UNGGE and OEWG were created for promoting stability in cyberspace. As these two processes continued in 2020 and are expected to produce results in 2021, the work completed in 2019 cannot be finished. Therefore, the 2020 BPF on Cybersecurity and this report continue the last years' efforts and specifically look into the norms development process from a broader perspective to identify baseline components which make norms happen and work as well as methods of norms assessment (when norms are adhered to or violated). For that we analyzed several case studies relying on key lessons learnt from the 2019 report[91], which reviewed how cybersecurity agreements are actioned and formulated with regard to purpose, value and outcome, as well as stakeholder actions that are fundamental to achieving an agreement's goals. Those lessons are:

Perceived value and outcome of cybersecurity agreements
Cybersecurity agreements may provide a valuable common footing to reduce risk and increase security and stability in cyberspace. Agreements may contribute to developing clear expectations for responsible behaviour, clarify responsibilities, increase the visibility and promotion of good cybersecurity practices, lay the basis for confidence-building measures between stakeholders and facilitate further cooperation and new partnerships.

Unintended adverse effects of cybersecurity agreements
Cybersecurity agreements may remain ineffective or even counterproductive. Unintended outcomes can often be traced back to causes within the agreement, the process and course of actions that led to the agreement. Cybersecurity agreements are at risk of becoming counterproductive when they limit multistakeholder input, fail to focus on outcomes but instead prescribe a particular course of action, miss the involvement of important global players, lack leadership in implementation, or directly or indirectly undermine human rights.

Common shortcomings
The success of a cybersecurity agreement largely depends on actions by its signatories and stakeholders. An agreement will facilitate actions if it is clear and unambiguous, defines key terminology early in the agreement, focuses on goals and avoids being overly prescriptive on implementation, makes awareness-

[91] The full report of the 2019 BPF Cybersecurity can be found at https://www.intgovforum.org/multilingual/filedepot_download/8395/1896

raising and capacity-building a crucial part of the agreement, foresees follow-up, monitoring and accountability mechanisms.
A lack of leadership in implementation, especially by influential actors, states, or those who called for the agreement, can undermine the success of an initiative.

Multistakeholder involvement in development and implementation
Including stakeholders in the design of norms and agreements can avoid needless ambiguity and the need to clarify language afterwards. Building networks where stakeholders can cooperate on implementation, or share how they are approaching the commitments and their implementation, allows to learn from peers and identify best practices. The assessment of norm adherence by Civil Society has contributed to establishing accountability and enumeration of responsible behaviours. This engagement can be a basis for other multistakeholder approaches.

Key conclusions from normative principles in global governance

In gathering lessons learned from the case studies above, we can glean the accepted elements of the successes of previous initiatives on process, content and implementation.

On process:
Practically speaking the success in diplomatic norms are due to the excellence of the preparatory work and negotiating skills that led to the Vienna Convention.

On content:
The success of the global nuclear norms regime stems from its concreteness.
In addition the long stability of the basic rules of diplomatic law. Controversial issues such as diplomatic asylum were avoided and exceptioned. World Bank Guidelines on Treatment of Foreign Direct Investment are technically rigourous.

On implementation and enforcement:
The effectiveness of the Vienna Convention is also due to the norm of reciprocity as a sanction against non-compliance. While the GSP perhaps only had widespread adoption and consensus because they lack concreteness, codification in binding documents and had few costs of violating those norms, they did give rise to more holistic frameworks for business ethics. The GSP could be considered as a launching pad for more legitimate and enforceable processes in local contexts.

PART II - Exploring Best Practices in Relation to International Cybersecurity Agreements

The IGF 2020 Best Practice Forum (BPF) on Cybersecurity's workstream focused on updating and further advancing the analysis of the 2019 BPF report on the state of international cybersecurity agreements, with a more narrow focus on cyber norms agreements, includes:

- Identifying new agreements and developments since last year to include in the analysis.
- Reviewing and refining the scope of agreements to be included in the report.
- Identifying a core group of agreements to include in the 2020 analysis.
- Identifying trends and commonalities between contents of cyber norms agreements.
- Releasing a call for contributions to gain further input on these selected agreements and their implementation.
- Updating last year's research paper with new learnings about implementation regarding these core agreements.

Authors

John R. Hering
Louise Marie Hurel
Frans van Aardt
YingChu Chen
Carina Birarda
Ayesha Khan
Wim Degezelle

Table of Contents

Scope of analysis – international agreements on cyber norms

In order to update the content of the 2019 BPF Cybersecurity report, a similar method was used in determining which international agreements would be included in the analysis for this year's report. We scoped agreements into the project based on the following criteria:

- The agreement describes specific commitments or recommendations that apply to any or all signatory groups (typically governments, non-profit organization or private sector companies);
- The commitments or recommendations must have a stated goal to improve the overall state of cybersecurity; and
- The agreement must be international in scope - it must have multiple well known actors that either operate significant parts of internet infrastructure, or are governments (representing a wide constituency).

In addition to these three criteria that were used in the previous BPF report, this year's report is also exclusively including in its analysis international agreements which *include voluntary, nonbinding norms for cybersecurity*, among and between different stakeholder groups. This is intended to help focus the analysis of the 2020 BPF, and the requests for contribution, on the impact of international agreements on cyber norms, areas of emerging consensus on cyber norms, and best practices for such efforts moving forward. It also will help to identify which norms are being more commonly included in different international agreements – said differently, *which norms are becoming "the norm" to include.* Agreements were identified by experts participating in the Best Practices Forum.

Classification of agreements

In our analysis, we classify agreements analysed under three headings:

- Agreements within the UN 1st Committee: We have chosen to situate the UN 1st Committee on international peace and security separately from the other agreements due to role the UN plays, and the position it holds as a multilateral forum which encompasses a wide range of state actors. It thereby plays a unique and high-level norm-setting role. Indeed, the cyber norms set out by the UN 1st Committee report serve as the foundation for our analysis of the other agreements in this report.

- Agreements within a stakeholder group: These can include agreements established in multilateral forums among states but also agreements among private sector or other nongovernmental actors.
- Agreements across stakeholder groups: These are often termed 'multistakeholder initiatives', and can include agreements which are led by a state actor but which include multiple stakeholders or non-governmental actors in their elaboration and implementation.

The agreements below between and among different stakeholder groups reflect the scope for analysis in this year's report. Building on the work of the 2019 BPF, it includes many of the same agreements included in the previous report, as well as new agreements and developments achieved over the past year. It does not include agreements which may have been included in the 2019 report but which are exclusively legally-binding or otherwise do not include specific voluntary cybersecurity norms.

Agreements included

In total, the BPF has identified 22 international agreements on cybersecurity norms for inclusion in this report, based on the scoping criteria above and split between three categories -- UN agreements, agreements within a stakeholder group, and agreements between multiple stakeholder groups.

UN Agreements

For this analysis, we have included the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security combined consensus reports from 2010/2013/2015, often referred to as the "The Framework for Responsible State Behavior in Cyberspace" – which includes the 11 norms featured in the 2015 consensus UN-GGE report.[92] The contents of the 2015 report, including its eleven norms, were formally adopted by the UN General Assembly in resolution 70/237[93], by consensus. The resolution "calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts."

A new iteration of the GGE – now labelled the GGE on "Advancing responsible State behaviour in cyberspace" – was established in 2019 through resolution 73/226 of the United Nations General Assembly, which will continue to explore these topics through 2021. The UNGGE has a narrow set of participants from UN member states, with 25 states included in the current body. As of 2019, there is also a new parallel UN initiative on these topics, established by resolution 73/27, the Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, which is open to the entire UN membership.

[92] https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[93] https://undocs.org/A/RES/70/237

The two bodies have had successive rounds of meetings across 2019 and 2020, including several informal sessions. Both the UNGGE and the OEWG are supported by the UN Office for Disarmament Affairs (UNODA). The General Assembly requested UNODA to collaborate with relevant regional organizations to convene a series of consultations that can provide input to the UNGGE process. In the case of the OEWG, the General Assembly requested UNODA to provide the possibility of holding an intersessional consultative meeting with interested parties, in particular business, nongovernmental organizations and academia, to share input on issues within the OEWG's mandate. This meting took place in December of 2019, at the UN headquarters in New York City.

Agreements within a single stakeholder group

Below are the agreements within stakeholder groups that are included in this report. These types of agreements, within a single stakeholder group (states, non-profits, private sector, academia, technical community, ...etc), were by far the most common form of cybersecurity norms-setting agreements we encountered in this initiative. They largely take advantage of existing institutions and forums, exclusive to certain stakeholders, in order to be established.

- The G20, in their Antalya Summit Leaders' Communiqué, noted that "affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors".
- The G7, in their Charlevoix commitment on defending Democracy from foreign threats, committed to "Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state."
- In 2017, the G7 also released its Declaration on Responsible States Behavior in Cyberspace, intended to promote "a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States."
- The Cybersecurity Tech Accord is a set of commitments promoting a safer online world through collaboration among technology companies.
- The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security frames cybersecurity approaches in a human rights context, and originates from a set of member governments.
- In the Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security, member states of the Shanghai Cooperation Organization agree on major threats to, and major areas of cooperation in cybersecurity.

- The Council to Secure the Digital Economy is a group of corporations which together published an International Anti-Botnet guide with recommendations on how to best prevent and mitigate the factors that lead to widespread botnet infections.
- The African Union Convention on Cyber Security and Personal Data Protection assists in harmonizing cybersecurity legislation across member states of the African Union.
- The League of Arab States published a Convention on Combating Information Technology Offences which intends to strengthen cooperation between the Arab States on technology related offenses.
- The East African Community (EAC) Draft EAC Framework for Cyberlaws contains a set of recommendations to its member states on how to reform national laws to facilitate electronic commerce and deter conduct that deteriorates cybersecurity.
- The Economic Community of Central African States' (ECCAS) 2016 Declaration of Brazzaville, aims to harmonize national policies and regulations in the Central African subregion.
- The NATO Cyber Defence Pledge, launched during NATO's 2016 Warsaw summit, initiated cyberspace as a fourth operational domain within NATO, and emphasizes cooperation through multinational projects.
- The EU Council's 2017 Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, which was published to all EU delegations, reinforced several existing EU mechanisms, such as the EU Cyber Security Strategy, and further recognized other instruments such as the Budapest Convention, while calling on all Member States to cooperate on cybersecurity through a number of specific proposals.
- The Mutually Agreed Norms for Routing Security (MANRS), an initiative by the Internet Society, is a voluntary set of technical good common practices to improve routing security compiled primarily by members of the network operators community, which has now expanded to include internet exchange points, as well.
- The Commonwealth Cyber Declaration, launched in 2018, is a commitment among the Commonwealth Heads of Government to "a cyberspace that supports economic and social development and rights online," "build the foundations of an effective national cybersecurity response," and "promote stability in cyberspace through international cooperation."

Multistakeholder agreements on cyber norms

Below are the multistakeholder cybersecurity agreements we included in this report. By comparison to agreements within stakeholder groups, multistakeholder agreements on cybersecurity norms and principles were found to be less common, and frequently reflect the output or launch of a new initiative to build cooperative relationships across stakeholder groups that have not previously existed.

- The Paris Call for Trust and Security in Cyberspace is a multistakeholder agreement on cybersecurity principles. It was launched by the French foreign ministry at IGF2018. It currently has over 1,000 official supporters, including 78 national governments.

- The Siemens Charter of Trust consists of private sector companies, in partnership with the Munich Security Conference, endorsing minimum general standards for cybersecurity through ten principles. Some of their associate members also include the German Federal Office for Information Security and Graz University of Technology.
- The Global Commission on the Stability of Cyberspace (GCSC) is a multi-stakeholder group of commissioners which together develop international cybersecurity related norms initiatives. Their most recent publication is a draft of Six Critical Norms, also known as the "Singapore Norms Package". It is a set of six new norms proposed by a multi-stakeholder group intended to improve international security and stability in cyberspace.
- The World Wide Web Foundation's Contract for the Web was launched in 2019 to create "a global plan of action to make our online world safe and empowering for everyone." The agreement includes roles for governments, organizations and individuals alike.
- Ethics for Incident Response and Security Teams (EthicsfIRST) is "designed to inspire and guide the ethical conduct of all Team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way." The initiative includes security teams across sectors.

Trends in international cyber norms

Due to the unique responsibility the United Nations has in matters of international peace and security, and the recognition of the GGE's 11 norms by consensus of the UN General Assembly, the BPF has used these norms as the basis for analysis of the other agreements included in this report. This was in an effort to determine whether or not these multilateral cyber norms are being recognized and reinforced in other agreements in order to be strengthened, implemented, or enforced – including with non-state stakeholders.

A team of expert contributors to the BPF on Cybersecurity reviewed each of the agreements included in this year's report in order to determine if they reflect any of the 11 cyber norms identified by the 2015 UN GGE consensus report. As various agreements apply to different stakeholder groups, and the GGE norms are written strictly to guide state behavior in cyberspace, the BPF used a simplified, up-leveled, version of each of the 11 UN cyber norms – focused on the resources being protected or the behavior being prohibited/promoted by the norm – when considering whether a similar norm existed in another agreement. The resulting simplified 11 norms considered include:

1. States should not allow territory be used for international wrongful acts via ICTs.
2. Do not conduct or support ICT activity that harms critical infrastructure.
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools.
4. Recognizing computer emergency response teams as a protected and benign group.
5. Recognizing human rights online and/or right to privacy.
6. Cooperation with states to increase stability and security in use of ICTs.
7. States (or other stakeholders) should consider all relevant information following ICT incidents.
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.
9. States (or other stakeholders) should protect their own critical infrastructure.
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.
11. Encourage responsible reporting of ICT vulnerabilities and share remedies.

The following charts reflect the frequency with which each of the 11 norms above have been reflected in each of the agreements included in the analysis, as determined by the team of experts. The sixth norm, calling for cooperation to promote stability and security in cyberspace, was the norm most commonly reflected in the other agreements, with some form of it being evident in 77% of the agreements reviewed. It is perhaps unsurprising that the norm most commonly found in such agreements states that there should be partnership and cooperation between the parties in the agreement. The next most frequently recognized norm was number five, which is reflected in 68% of the agreements and recognizes of either human rights or privacy rights online. States preventing their own territory from being used in wrongful ICT acts, norm number one, was the UN norm least often reflected in other agreements.

A note on the charts below and the analysis:

Comparing international agreements across regions, and stakeholder groups, necessarily requires that those conducting the analysis make informed assumptions about intentions and meaning in different agreements. It also requires an expansive understanding of each of the norms included, in order to capture when they are reflected in other agreements. Indeed, language reflecting the 11 GGE norms was often found within the preamble of an agreement, or as part of another norm entirely. While the specific language in international agreements is generally carefully crafted and highly intentional, the analysis here focuses less on the specific language and more on the spirit of the norm itself. After all, a norm by definition is not an explicitly defined rule with narrow boundaries but a general principle to be adhered to.

In addition, while the analysis here focuses on the 11 norms established by the UN-GGE for the reasons described above, this is not meant to imply causality or influence in terms of why similar norms are included in other agreements. Several of the agreements included below actually pre-date the 2015 UN-GGE report, so their content could not have been influenced by that report. In fact, it is possible that they would have been influencers of the GGE. Of course, other agreements may have simply independently reached similar conclusions about what norms should be established in cyberspace.

Chart I: frequency of each norm in other agreements

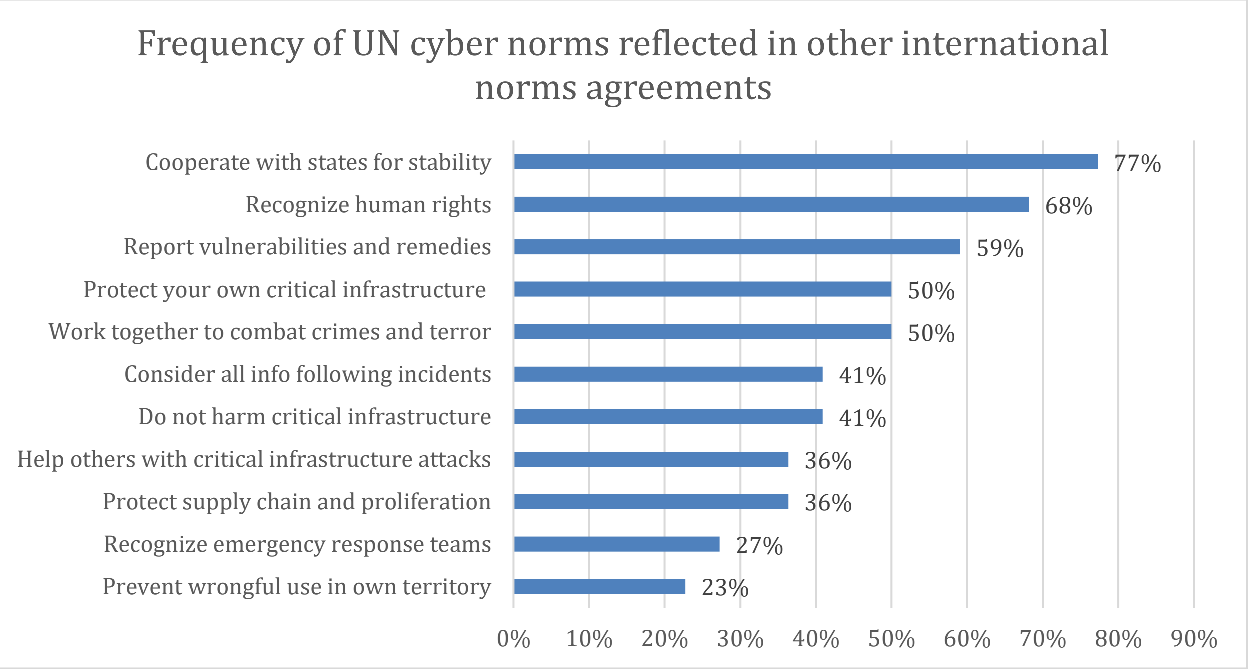


Chart II – UN Cyber norms reflected in each agreement

UN cyber norms reflected in international cybersecurity agreements

	International Agreements	Simplified UN Cyber Norms										
		#1 Prevent wrongful use in territory	#2 Do not harm critical infrastructure	#3 Protect supply chain & against proliferation	#4 Recognize emergency response teams	#5 Recognize human rights/privacy	#6 Cooperate with states for stability	#7 Consider all info following incidents	#8 Work together to combat criminals & terorrists	#9 Protect your own critical infrastructure	#10 Help others with critical infrastructure attacks	#11 Report vulnerabilities and remedies
1	The G20 Antalya Summit Leaders' Communiqué	○	○	○	○	●	○	○	○	○	○	○
2	The G7 Charlevoix commitment on defending Democracy from foreign threats	○	○	○	○	○	●	○	○	○	○	○
3	G7 Declaration on Responsible States Behavior in Cyberspace	●	●	●	●	●	●	●	●	●	●	●
4	The Cybersecurity Tech Accord	○	○	●	○	○	●	○	●	○	○	●
5	The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to cybersecurity	○	○	○	○	●	○	○	○	○	○	○
6	Shanghai Cooperation Organization Agreement on cooperation in international information security	○	○	○	○	○	●	●	●	●	○	○
7	The African Union Convention on Cyber Security and Personal Data Protection	●	●	●	○	●	●	○	●	●	●	●
8	The Council to Secure the Digital Economy International Anti-Botnet guide	○	●	○	●	●	●	●	○	○	●	●
9	The League of Arab States Convention on Combating Information Technology Offences	●	●	○	○	●	●	●	●	●	●	○
10	The East African Community (EAC) Draft EAC Framework for Cyberlaws	○	○	○	○	●	●	○	○	○	○	○
11	The Economic Community of Central African States (ECCAS) Declaration of Brazzaville	○	○	○	●	○	●	○	○	○	○	○
12	The NATO Cyber Defence Pledge	●	●	●	○	●	●	●	●	●	●	●
13	The EU Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	○	○	○	○	●	●	●	○	●	○	●
14	The Mutually Agreed Norms for Routing Security (MANRS)	○	○	○	○	○	○	○	●	○	○	●
15	The Southern African Development Community Model Laws on Cybercrime	○	●	○	○	○	○	○	○	○	○	○
16	The Paris Call for Trust and Security in Cyberspace	○	●	●	○	●	●	○	○	●	●	●
17	UN-GGE 2015 consensus report*	●	●	●	●	●	●	●	●	●	●	●
18	The Siemens Charter of Trust"	○	○	●	○	○	●	○	●	●	○	○
19	GCSC's Six Critical Norms	○	●	●	○	●	●	●	●	●	○	●
20	Commonwealth Cyber Declaration	○	○	○	●	●	●	○	○	●	●	●
21	World Wide Web Foundation's Contract for the Web	○	○	○	○	●	●	○	○	○	○	●
22	Ethics for Incident Response and Security Teams (EthicsfIRST)	○	○	○	●	●	○	●	●	○	○	●

*all norms are reflected in the 2015 UN-GGE report

Analysis of Agreements

Each of the international cybersecurity agreements featuring cyber norms identified above is reviewed below based on i) when they were initiated, ii) which stakeholders are included, iii) the total number of supporters/signatories, iv) whether there is an organization responsible for maintaining the agreement, v) whether any of the eleven UN-GGE norms are reflected in the agreement, and vi) what other norms are featured.

#	**Agreement** (links included as available)
I.	The G20 Antalya Summit Leaders' Communiqué
II.	The G7 Charlevoix commitment on defending Democracy from foreign threats
III.	G7 Declaration on Responsible States Behavior in Cyberspace
IV.	The Cybersecurity Tech Accord
V.	The Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security
VI.	In the Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security
VII.	The African Union Convention on Cyber Security and Personal Data Protection
VIII.	The Council to Secure the Digital Economy International Anti-Botnet guide
IX.	The League of Arab States Convention on Combating Information Technology Offences
X.	The East African Community (EAC) Draft EAC Framework for Cyberlaws
XI.	The Economic Community of Central African States (ECCAS) Declaration of Brazzaville
XII.	The NATO Cyber Defence Pledge
XIII.	The EU Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
XIV.	The Mutually Agreed Norms for Routing Security **(**MANRS**)**
XV.	The Southern African Development Community Model Laws on Cybercrime
XVI.	The Paris Call for Trust and Security in Cyberspace
XVII.	UN Group of Governmental Experts (GGE) on information security combined consensus reports from 2010/2013/2015 – "The Framework for Responsible State Behavior in Cyberspace" – which includes the 11 norms featured in the 2015 consensus report.
XVIII.	The Siemens Charter of Trust"
XIX.	GCSC's Six Critical Norms
XX.	Commonwealth Cyber Declaration
XXI.	World Wide Web Foundation's Contract for the Web
XXII.	Ethics for Incident Response and Security Teams (EthicsfIRST)

I. G20 Leaders' Communiqué, Antalya Summit

A. Date it was signed/launched: November, 2015

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 19 member-states.

D. Organization responsible for the agreement: G20

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

The Communiqué welcomes the 2015 report of the GGE and affirms that "international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45."

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure**. N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.** Yes**.**

   "All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications."
6. **Cooperation with states to increase stability and security in use of ICTs**. – N/A
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. **–** N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** – N/A
9. **States (or other stakeholders) should protect their own critical infrastructure.** – N/A
10. States **(or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** – N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** – N/A

F. Additional norms included in the agreement:

"[W]e affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

II. G7 Declaration on Responsible States Behavior in Cyberspace

A. Date it was signed/launched: April, 2017

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 7 Countries

D. Organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

IMPORTANT*: The Lucca Declaration restates **all 2015 GGE** norms and 2015 G20 Leaders' Communiqué, quoting the resolution/communiqué. That repetitive norms language is reflected below in red. Meanwhile, in black are references reflected in other sections of the document and that might contain a different approach or nuance than the list of norms at the end of the document.

1. **States should not allow territory be used for international wrongful acts via ICTs**

   States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

2. **Do not conduct or support ICT activity that harms critical infrastructure**.

   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;

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.**

   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;

4. **Recognizing computer emergency response teams as a protected and benign group.**

   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.

5. **Recognizing human rights online and/or right to privacy**

   Indirect reference to the UNGA Resolution on the Right to Privacy in the Digital Age: "*We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties".*

   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;

6. **Cooperation with states to increase stability and security in use of ICTs**

   "*We recognize the urgent necessity of increased international cooperation to promote security and stability in cyberspace, including on measures aimed at reducing the malicious use of ICTs by State and non-State actors".*

   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;

7. **States (or other stakeholders) should consider all relevant information following ICT incidents.**

   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; 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;

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs;**

   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;

9. **States (or other stakeholders) should protect their own critical infrastructure**

   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;

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.**

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;

11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**
    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;

F. Additional norms included in the agreement:

It should be noted that, unlike other declarations that only reinforce their commitment to the GGE 2015 norms, the Lucca Declaration of the G7 indicates a future pathway of commitment towards the promotion of "a strategic framework for conflict prevention, cooperation and stability in cyberspace" that observes the applicability of IL to state behavior in cyberspace, promotion of voluntary, non-binding norms of responsible State behavior during peacetime and the implementation and development of CBMs.

- Specific note on cyber attribution: *"We note that the customary international law of State responsibility supplies the standards for attributing acts to States, which can be applicable to activities in cyberspace. In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies […] In this context, a State assesses the facts and is free to make its own determination in accordance with international law with respect to attribution of a cyber-act to another State;"*
- Calls for public explanation from states on how IL applies to cyberspace.
- Refers to 2016 G7 document on "Principles and Actions on Cyber" that recognized the right of states to exercise collective or individual self-defense in accordance with Art. 51 of the UN Charter: "*We also recognized that States may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace;"*
- Endorses CBMs as an "essential element to strengthen international peace and security".
- Calls against intellectual property theft and espionage; "No country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

Not necessarily a norm, but more of a general comment. The G7 Lucca Declaration highlights member-states' position on what norms are and their importance for international cybersecurity:

> "In addition, we support the promotion of voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime, which can reduce risks to international peace, security and stability. Such norms do not seek to limit or prohibit any action that is otherwise consistent with international law. Nor do norms limit a State's obligations under international law, including with regard to human rights**. Norms reflect the current expectations of the international community, set standards for responsible State behavior, and allow the international community to assess the activities and intentions** of States. **Norms can help to prevent conflict in the ICT environment** and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development."

III. G7 Charlevoix Commitment on Defending Democracy from Foreign Threats

A. Date it was signed/launched: June, 2018

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 7 member-states.

D. Organization responsible for the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs**. N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure**. N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.** N/A
6. **Cooperation with states to increase stability and security in use of ICTs.** Yes.

   Establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

   Strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state.
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure.** N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack**. N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** N/A

F. Additional norms included in the agreement:

It calls for cross-sector collaboration in sharing lessons and best practices in promoting a peaceful, stable, secure and rights-respecting approach to defending democracy against foreign threats: *"Share lessons learned and best practices in collaboration with governments, civil society and the private sector that are developing related initiatives including those that promote free, independent and pluralistic media; fact-based information; and freedom of expression."*

It also singles out ISPs and social media platforms as key actors in information sharing practices to ensure privacy and prevention of illegal use of personal data: *"Engage directly with internet service providers and social media platforms regarding malicious misuse of information technology by foreign actors, with a particular focus on improving transparency regarding the use and seeking to prevent the illegal use of personal data and breaches of privacy."*

Given the scope of the Charlevoix Commitment, G7 countries also endorsed the following norms:

- Media literacy/Education: *Support public learning and civic awareness aimed at promoting critical thinking skills and media literacy on intentionally misleading information, and improving online security and safety.*
- Transparency in reporting during elections: *In accordance with applicable laws, ensure a high level of transparency around sources of funding for political parties and all types of political advertising, especially during election campaigns.*

IV. Cybersecurity Tech Accord

A. Date it was signed/launched: April, 2018

B. Stakeholders who are party to the agreement: Industry – Technology Industry.

C. Total number of signatories/supporters of the agreement: 145

D. Organization responsible for the agreement: There is a secretariat responsible for managing the agreement and its efforts.

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools**. Yes**.**
   We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.** N/A
6. **Cooperation with states to increase stability and security in use of ICTs.** Yes
   We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.
7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes
   We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.
9. **States (or other stakeholders) should protect their own critical infrastructure.** N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**. Yes.
    We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.

F. Additional norms included in the agreement:

1. We will protect all of our users and customers everywhere.
   a. We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.
   b. We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.
2. We will oppose cyberattacks on innocent citizens and enterprises from anywhere.
   a. We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.
3. We will help empower users, customers and developers to strengthen cybersecurity protection.
   a. We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
4. We will partner with each other and with likeminded groups to enhance cybersecurity.

V. Freedom Online Coalition

A. Date it was signed/launched: September 2015

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 32

D. Organization responsible for the agreement: Freedom Online Coalition

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A

2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools**. N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy. Yes.**

   1) Cybersecurity policies and decision-making processes should protect and respect human rights.

   2) The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.

   4) The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law

   5) Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy

   6) Responses to cyber incidents should not violate human rights.

   8) Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy."

   9) Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.

   10) Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.

   11) Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.

   12) Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders.

   13) Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity
6. **Cooperation with states to increase stability and security in use of ICTs**. N/A
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure**. N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**. N/A

F. Additional norms included in the agreement: N/A

VI. Agreement in Ensuring International Information Security Between Member States of the Shanghai Cooperation Organization.

A. Date it was signed/launched: June, 2009

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: 6

D. Organization responsible for ongoing management of the agreement: Shanghai Cooperation Organization

E. Norms adapted from 2015 UN-GGE consensus report reflected in the agreement

Even though the SCO Agreement precedes the GGE report, it does mention the UNGA on "Developments in the field of information and telecommunications in the context of international security" – probably the latest report A/RES/63/37 Jan 2009.

Overall, the agreement establishes the conditions through which information security cooperation should be conducted in the SCO. It provides a list of common key threats and *basic* threats (annex) to international information security (Art. 2), establishes main areas, principles, formats and mechanisms for collaboration and specifications on the protection of information, funding and relationship of the agreement with other international treaties.

1. States should not allow territory be used for international wrongful acts via ICTs **– N/A**
2. Do not conduct or support ICT activity that harms critical infrastructure. – **N/A**
3. Protections for ICT supply chain security, preventing the spread of malicious ICT tools. – **N/A**
4. Recognizing computer emergency response teams as a protected and benign group. – **N/A**
5. Recognizing human rights online and/or right to privacy – **N/A**
6. Cooperation with states to increase stability and security in use of ICTs – **Yes**
    - *defining, coordinating and implementing necessary joint measures in the field of ensuring international information security; (Art. 3)*
    - *conducting expertise, research and evaluation in the field of information security necessary for the purposes of this Agreement; (Art. 3)*
    - *promoting secure, stable operation and governance internationalization of the global Internet network; (Art. 3)*
    - *creating of a system of joint monitoring and response to emerging threats in this area; (Art. 3)*
    - *developing and implementing joint measures of trust conducive to ensuring international information security*
7. States (or other stakeholders) should consider all relevant information following ICT incidents – **Yes**
    - *exchanging information on issues related to the cooperation in the basic areas listed in this Article (Art.3)*
8. States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs. – **Yes**
    - *[SCO parties shall cooperate in] countering threats related to the use of information and communication technologies for terrorist purposes (Art. 3)*
    - *Combatting cybercrime (Art.3)*
9. States (or other stakeholders) should protect their own critical infrastructure – **Yes**
    - ensuring information security of the critically significant structures of the Parties (Art.3)
10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack – **N/A**
11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **N/A**

F. Additional norms included in the agreement:

- Capacity building:
    - exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized representatives and experts of the Parties in the field of information security; (Art. 3(15))
    - creating conditions for cooperation between the competent authorities of the Parties in order to implement this Agreement (Art. 3(13)).
- Data protection and cross-border data flows: developing and implementing coherent policies and organizational and technical procedures for the implementation of digital signature and data protection in the cross-border exchange of information (Art.3(10))
- More on cooperation and knowledge exchange:
    - exchanging information on the legislation of the Parties on issues of information security (Art.3(11)).
    - interacting within international organizations and fora on issues of international information security (Art.3(14))

  - elaborating joint measures for the development of the provisions of the international law limiting the spread and use of information weapons threatening defense capacity, national security and public safety (Art.3(3)).
- Cooperation will be conducted in a way that is consistent "with universally recognized principles and norms of the international law, including the principles of peaceful settlement disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of regional cooperation and non- interference in the information resources of the Parties" (Art.4 (1)).

VII. African Union Convention on Cyber Security and Personal Data Protection

A. Date it was signed/launched: June 2014

B. Stakeholders who are party to the agreement: Governments in Africa

C. Total number of signatories/supporters of the agreement: 14/55 Signed 8/55 Ratified and Deposited

D. Organization responsible for the agreement: African Union

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** Yes
   - *Article 29*
   - *Offences specific to Information and Communications Technologies*
   - *"Participate in an association formed or in an agreement established with a view to preparing or committing one or several of the offences provided for under this Convention."*
2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes
   - *Article 25*
   - *" 4. Protection of Critical Infrastructure*
   - *Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management."*
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** Yes
   - *Article 29*
   - *Offences specific to Information and Communications Technologies*
   - *"g. Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers;*
   - *h. Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or specially adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing access to part or all of a computer system"*
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.** Yes.
   - *Article 25*
   - *"In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions,*

particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others."

6. **Cooperation with states to increase stability and security in use of ICTs**. Yes.
    - *Article 28*
    - *International cooperation*
    - *" 1. Harmonization*
    - *State Parties shall ensure that the legislative measures and/or regulations adopted to fight against cyber-crime will strengthen the possibility of regional harmonization of these measures and respect the principle of double criminal liability."*
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes.
    - *Article 28*
    - *International Cooperation*
    - *"2. Mutual legal assistance*
    - *State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis."*
9. **States (or other stakeholders) should protect their own critical infrastructure. Yes.**
    - *Article 25*
    - *" 4. Protection of Critical Infrastructure*
    - *Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management."*
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** Yes (indirectly).
    - *Article 28*
    - *International Cooperation*
    - *" 2. Mutual legal assistance*
    - *State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis."*
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** Yes.
    - *Article 29*
    - *Offences specific to Information and Communications Technologies*
    - *"g. Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerabilities detected and the solutions recommended to correct them to consumers;"*

F. Additional norms included in the agreement:

<u>Promotion of Cybersecurity Governance</u>

"Article 27

National cyber security monitoring structures

Cyber security governance

a) Each State Party shall adopt the necessary measures to establish an appropriate institutional mechanism responsible for cyber security governance;

b) The measures adopted as per paragraph 1 of this Article shall establish strong leadership and commitment in the different aspects of cyber security institutions and relevant professional bodies of the State Party. To this end, State Parties shall take the necessary measures to:

i. Establish clear accountability in matters of cyber security at all levels of Government by defining the roles and responsibilities in precise terms;

Express a clear, public and transparent commitment to cyber security;

Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.

c) Cyber security governance should be established within a national framework that can respond to the perceived challenges and to all issues relating to information security at national level in as many areas of cyber security as possible."

<u>Promote Multi stakeholder</u>

"Article 26

National cyber security system

1. Culture of Cyber Security

a) Each State Party undertakes to promote the culture of cyber security among all stakeholders, namely, governments, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks. The culture of cyber security should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using information systems as well as during communication or transactions across networks.

b) As part of the promotion of the culture of cyber security, State Parties may adopt the following measures: establish a cyber-security plan for the systems run by their governments; elaborate and implement programmes and initiatives for sensitization on security for systems and networks users; encourage the development of a cyber-security culture in enterprises; foster the involvement of the civil society; launch a comprehensive and detailed national sensitization programme for Internet users, small business, schools and children.

3. Public-Private Partnership

Each State Party shall develop public-private partnership as a model to engage industry, the civil society, and academia in the promotion and enhancement of a culture of cyber security."

<u>Confidence Building Measures</u>

"Article 26

National cyber security system

2. Role of Governments

Each State Party shall undertake to provide leadership for the development of the cyber security culture within its borders. Member States undertake to sensitize, provide education and training, and disseminate information to the public.

4. Education and training

Each State Party shall adopt measures to develop capacity building with a view to offering training which covers all areas of cyber security to different stakeholders, and setting standards for the private sector.

States Parties undertake to promote technical education for information and communication technology professionals, within and outside government bodies, through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material."

VIII. The Council to Secure the Digital Economy International Anti-Botnet guide (2018 & 2020)

A. Date it was signed/launched: Initial document was finished in November 2018, while the latest one on their website was finished in November 2019 (2020)

B. Stakeholders who are party to the agreement: Industry

C. Total number of signatories/supporters of the agreement: 14 enterprises / companies

D. Organization responsible for the agreement: Council to Secure the Digital Economy (CSDE)

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

   The global economy, critical infrastructure and government operations have increased their dependence on software.

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** Yes

   REAL-TIME INFORMATION SHARING*: Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information. Examples include information from government and law enforcement information sharing activities, various CERTs, industry groups, network providers, RFC2142 addresses, and updates and alerts from vendors and other sources. (2018/ P.34; 2020/p.41)*

5. **Recognizing human rights online and/or right to privacy.** Yes.

   Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. (2018/p. 36; 2020/p.44)

6. **Cooperation with states to increase stability and security in use of ICTs. Yes.**
   - *They are able to work in partnership with government and industry to take down malicious botnets. They may also offer commercial services such as scrubbing traffic and DDoS protection. (2018/p.18; 2020/p.23)*
   - *Threat modeling and analysis of risks to architecture: Companies that work with governments or whose operations are highly sensitive may hire teams of experts to determine how malicious actors would hypothetically create or exploit vulnerabilities in a system to achieve nefarious ends. A threat model may consider many types of risks, including those involving automated, distributed attacks. (2018/p.24; 2020/p29)*
7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** Yes.

   The entirety of the "secure-by-design" section.

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure.** N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** Yes.

    Enterprises should be prepared to receive and act responsively and responsibly upon cyber threat information provided by information sharing activities even when not yet committed to actively share information.(2018/p.34; 2020p.41)

11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** Yes.

Enterprises should maintain contact with sharing communities and be aware of the processes and safeguards to properly report/share cyber security incidents within their region and industry. (2018/p.34; 2020/p.42)

F. Additional norms included in the agreement: N/A

IX. Arab Convention on Combating Information Technology Offences[94]

A. Date it was signed/launched: Adopted on 21 December 2010 and came into force in 2014 (after the ratification of seven states).[95]

B. Stakeholders who are party to the agreement: Governments **–** Jordan, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, United Arab Emirates, Tunisia, Algeria, Djibouti, Sudan, Syria, Somalia, Iraq, Palestine, Comoros, Lebanon, Libya, Egypt, Morocco, Mauritius and Yemen.

C. Total number of signatories/supporters of the agreement: 22

D. Organization responsible for the agreement: General Secretariat of the Council of Arab Interior Ministers (CAIM) and the Technical Secretariat of the Arab Justice Ministers.

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs. Yes.**
    a) *Desiring to enhance cooperation between themselves to combat information technology offences threatening their security, interests and the safety of their communities, (Preamble)*
    b) *Convinced of the need to adopt a common criminal policy aimed at protecting the Arab society against information technology offences, (Preamble)*
    c) *to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals. (Preamble)*
    d) ***Article 9**: **Offence of Misuse of Information Technology Means** (1)- The production, sale, purchase, import, distribution or provision of: a- any tools or programmes designed or adapted for the purpose of committing the offences indicated in Articles 6 to 8. b- the information system password, access code or similar information that allows access to the information system with the aim of using it for any of the offences indicated in Articles 6 to 8. (2)- The acquisition of any tools or programmes mentioned in the two paragraphs above with the aim of using them to commit any of the offences indicated in Articles 6 to 8.*
2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

    ***Article 6: Offense of Illicit Access**: (1)- Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. (2)- The punishment shall be increased if this access, presence, contact or perpetuation leads to: a- the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries. b- the acquirement of secret government information*
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy**. **Yes.**
    a) *Adhering to the relevant Arab and international treaties and charters on human rights, and guaranteeing, respecting and protecting them (Preamble)*

[94] https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab Convention on Combating Information Technology Offences.pdf

[95] https://www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf , and https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh.pdf

b) ***Article 14**: **Offence Against Privacy** - Offence against privacy by means of information technology*

6. **Cooperation with states to increase stability and security in use of ICTs. Yes.**

   a) *The purpose of this convention is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals (Preamble)*

7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** Yes.

   a) ***Article 28: Expeditious Gathering of Users Tracking Information** – (1)- Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to: a- gather or register using technical means in the territory of this State Party. b- require the service provider, within his technical competence, to: - gather or register using technical means in the territory of this State Party, or - cooperate with and help the competent authorities to expeditiously gather and register users tracking information with the relevant communications and which are transmitted by means of the information technology. (2)- If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of users tracking information corresponding to the relevant communications in its territory using the technical means in that territory. (3)- Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.*

   b) ***Article 33 - Circumstantial Information:** (1)- A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. (2)- Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.*

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes.

   ***Article 32: Mutual Assistance** – (1)- All State Party shall lend assistance to each other to the fullest extent for the purposes of investigation, procedures related to information and information technology offences or to gather electronic evidence in offences.*

9. **States (or other stakeholders) should protect their own critical infrastructure.** Yes.

   a) ***Article 5: Criminalization** - Every State Party shall commit itself to the criminalization of acts set forth in this chapter, according to its legislations and statutes.*

   b) ***Article 21: Increasing Punishment for Traditional Crimes Committed by Means of Information Technology** - Every State Party shall commit itself to increasing the punishment for traditional crimes when they are committed by means of information technology*

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** Yes.

    Article 32: Mutual Assistance – (1)- All State Party shall lend assistance to each other to the fullest extent for the purposes of investigation, procedures related to information and information technology offences or to gather electronic evidence in offences.

11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** N/A.

F. Additional norms included in the agreement:

1) Sovereignty:

   i. ***Article 4: Safeguarding Sovereignty** - (1)- Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non-interference in the internal affairs of other States.*

ii. ***Article 35: Refusal of Assistance*** *- In addition to the grounds for refusal set forth in Article 32, paragraph 4, the State Party from which assistance is requested may refuse assistance if: 1- the request relates to an offence that the law of the State Party from which assistance is requested considers as a political offence. 2- It considers that implementing the request could constitute a violation of its sovereignty, security, order or basic interests.*

2) Principles of Sharia Law as a Determinative Legal Framework:

iii. *Taking into account the high religious and moral principles, especially the ordinances of Islamic Law (Shari'a), as well as the human heritage of the Arab Nation which rejects all forms of crimes, and having regard to public order in every State. (Preamble)*

X. AC Framework for Cyberlaws

A. Date it was signed/launched: May 2010

B. Stakeholders who are party to the agreement: Governments in East African Community - Burundi, Kenya, Rwanda, Tanzania, and Uganda

C. Total number of signatories/supporters of the agreement: 5

D. Organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group. N/A**
5. **Recognizing human rights online and/or right to privacy.** Yes.
   - *"The Task Force recognises the critical importance of data protection and privacy and recommends that further work needs to carried out on this issue, to ensure that (a) the privacy of citizens is not eroded through the Internet.*
   - *2.5Data Protection and Privacy For the purposes of the Framework, 'data protection' is used here to describe those obligations placed upon those entities that process information about living individuals, generally referred to as 'personal data'. A data protection regime will also grant certain rights upon individual data subjects. The application of data protection rules may be limited only to private sector entities or public bodies. A sectoral regulatory response may be appropriate to address specific uses and abuses of personal data, whether driven by domestic or foreign concerns, such as the financial services sector. In terms of the entity responsible for the processing, the following minimum obligations represent international best practice in the area:*
   - *18 •To comply with certain 'principles of good practice' in respect of their processing activities, including accountability, transparency, fair and lawful processing, processing limitation, data accuracy and data security. •To supply the individual with a copy of any personal data being held and processed and provide an opportunity for incorrect data to be amended."*
6. **Cooperation with states to increase stability and security in use of ICTs.** Yes.
   - *"The purpose of developing a Cyberlaw Framework for the EAC Partner States is to promote regional harmonisation in the legal response to the challenges raised by the increasing use and reliance on ICT for commercial and administrative activities, specifically in an Internet or cyberspace environment. Such a Framework details those agreed features that should be transposed into national laws and regulations in order to address the various issues identified in respect of the five topics discussed below. These features will include matters that are considered part of an essential response to a specific problem, as well as matters on which the Partner States may optionally choose to adopt measures."*
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure**. N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** N/A

F. Additional norms included in the agreement: N/A

XI. Declaration of Brazzaville

A. Date it was signed/launched: November 2016

B. Stakeholders who are party to the agreement: Governments [Member States of the Economic Community of States of Central Africa (ECCAS)]

C. Total number of signatories/supporters of the agreement: 11

D. Is there an organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** Yes.
   - *To support member states in setting up Centers for National Cyber Incident Alerts and Response (CIRT) and in the constitution of a sub-regional CIRT;"*
5. **Recognizing human rights online and/or right to privacy.** N/A
6. **Cooperation with states to increase stability and security in use of ICTs.** Yes.

   "1.To support member states in the process of transposing Model laws relating to Telecommunications / ICT and cybersecurity

   2. To facilitate the development of a regulatory reference framework cross-border interconnection;

   3. To support member states in the process of Strengthening capacities and development of Human Resources in terms of cybersecurity;

   4. Support member states in setting up CIRTs national and a sub-regional CIRT;

   5. To assist member states in setting up programs of child protection"
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure**. N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack**. N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** N/A

F. Additional norms included in the agreement: N/A

Confidence Building Measures "To institute awareness campaigns for the whole of the population to the culture of cybersecurity;To promote the establishment of training courses in cybernetics.

XII. NATO - Cyber Defense Pledge

A. Date it was signed/launched: Jul, 2016

B Stakeholders who are party to the agreement: Allied Heads of State and Governments

C. Total number of signatories/supporters of the agreement: NATO is an alliance that consists of 30 independent member countries

D. Organization responsible for the agreement: NATO, e-mail information not available.

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** Yes.

    ”1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.”

2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

    ”2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.”

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** Yes.

    ” 5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO’s cyber defence capabilities, as part of NATO’s long term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance.”

4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy**.

    ”We reaffirm the applicability of international law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and confidence-building measures in cyberspace.”

6. **Cooperation with states to increase stability and security in use of ICTs.**

    ” I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks; deepen co-operation and the exchange of best practices;”

7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** Yes.

    ”V. Improve our understanding of cyber threats, including the sharing of information and assessments.”

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs**. Yes.

    4. We emphasise NATO’s role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.

9. **States (or other stakeholders) should protect their own critical infrastructure.** Yes.

    5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority.

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** Yes.

    NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to full its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.

11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** Yes.
    - *We emphasise NATO's role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence eorts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.*
    - *IV. Improve our understanding of cyber threats, including the sharing of information and assessments;*

F. Additional norms included in the agreement:

Article 3 of the Washington Treaty

XIII. Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defense: Building strong cybersecurity for the EU

A. Date it was signed/launched: September, 2017

B. Stakeholders who are party to the agreement: Governments

C. Total number of signatories/supporters of the agreement: N/A

D. Organization responsible for ongoing management of the agreement: European Union

E. Norms adapted from 2015 UN-GGE consensus report included in the agreement

The Joint statement is a summary of the different initiatives set out by the EU to enhance cyber resilience. With that in mind, it provides a perspective on best practices in operationalizing some of the 2015 GGE norms while restating some of the guiding principles and policy documents guiding this strategic vision of cybersecurity within the Digital Single Market – therefore a bit beyond the scope of the exercise here. Other docs such as the NIS directive, Cybersecurity Act or Blueprint for coordinated cyber attack response. I've added a couple of examples related to the norms below.

However, it also does explicitly endorse the GGE voluntary non-binding norms: "The EU strongly promotes the position that international law, and in particular the UN Charter, applies in cyberspace. As a complement to binding international law, the EU endorses the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts84; it also encourages the development and implementation of regional confidence building measures, both in the Organisation for Security and Co-operation in Europe and other regions."

1. **States should not allow territory be used for international wrongful acts via ICTs**. N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.**

   The EU will prioritise international security issues in cyberspace in its international engagements, while also ensuring that cybersecurity does not become a pretext for market protection and the limitation of fundamental rights and freedoms, including the freedom of expression and access to information. A comprehensive approach to cybersecurity requires respect for human rights, and the EU will continue to uphold its core values globally, building on the EU's Human Rights Guidelines on online freedom. In that regard, the EU emphasises the importance of all stakeholders' involvement in the governance of the internet.

6. **Cooperation with states to increase stability and security in use of ICTs.**

A rapid and shared understanding of threats and incidents as they unfold is a prerequisite for deciding whether joint mitigation or response action supported by the EU is needed. Such information exchange requires the involvement of all relevant actors – EU bodies and agencies, as well as Member States – at technical, operational and strategic levels. ENISA, in cooperation with the relevant bodies at Member State and EU level, notably the network of Computer security incident response teams, CERT-EU, Europol and the EU Intelligence and Situation Centre (INTCEN), will also contribute to EU-level situational awareness.

7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. **Yes.**

   Countering hybrid threats: *The EU and NATO will also foster cyber defence research and innovation cooperation, andbuild on the current technical arrangement on cybersecurity information sharing between their respective cybersecurity bodies.*

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure. Yes.**

   The EU cybersecurity certification framework would operate as a voluntary scheme whereby all 'relevant stakeholders' would be called to take measures to deal with the evolving cybersecurity landscape – paying attention to the preservation of 'essential services' (transport, energy, health care, banking, financial market infrastructures, drinking water or digital infrastructure).

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack**. N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**. Yes.

    Mentioned under the wider objective of the establishment of an EU cybersecurity certification framework. The Joint communication document recognizes the important role of third party security researchers in discovering vulnerabilities and notes that "conditions to enable coordinated vulnerability disclosure should be created across Member States, building on best practice and relevant standards."

F. Additional norms included in the agreement:

Reinforces the role of cyber capacity building for global cyber stability: *The EU will continue to promote a rights-based capacity building model, in line with the Digital4Development approach. The priorities for capacity-building will be the EU's neighborhood and developing countries experiencing fast growing connectivity and rapid development of threats. EU efforts will be complementary to the EU's development agenda in light of the 2030 Agenda for Sustainable Development and overall efforts for institutional capacity building.*

XIV. Mutually Agreed Norms for Routing Security (MANRS)

A. Date it was signed/launched: 2014 (Current version 2.3 updated Sept. 2019)

B. Stakeholders who are party to the agreement: Multistakeholder Network Operators, Internet Exchange Points (IXPs), and Content Delivery Networks (CDNs)

C. Total number of signatories/supporters of the agreement: 528 total members

- 460 – Network Operators
- 56 – IXPs
- 12 – CDN & Cloud Providers

D. Organization responsible for the agreement: The Internet Society

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory to be used for international wrongful acts via ICTs.** N/A

2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.** N/A
6. **Cooperation with states to increase stability and security in use of ICTs**. N/A
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes.
    a. CDN & Cloud Providers – "Facilitate global operational communication and coordination"
    b. IXP's – "Facilitate global operational communication and coordination between network operators."
    c. Network Operators – "Coordination – Maintain globally accessible up-to-date contact information"
9. **States (or other stakeholders) should protect their own critical infrastructure.** N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack**. N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**. Yes.

    IXP's – "Action 5. Provide monitoring and debugging tools to the members."

F. Additional norms included in the agreement:

CDN & Cloud Providers actions:

- Prevent propagation of incorrect routing information
- Prevent traffic of illegitimate source IP addresses
- Facilitate validation of routing information on a global scale
- Encourage MANRS adoption
- Provide monitoring and debugging tools to peering partners (optional)

IXP Actions:

- Action 1. Prevent propagation of incorrect routing information. (Mandatory)
- Action 2. Promote MANRS to the IXP membership.
- Action 3. Protect the peering platform.
- Action 4. Facilitate global operational communication and coordination between network operators.

Network operator actions:

- **Filtering** – Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity
- **Anti-spoofing** – Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure
- **Coordination** – Maintain globally accessible up-to-date contact information
- **Global Validation** – Publish your data, so others can validate routing information on a global scale

XV. Southern Africa Model Laws

A. Date it was signed/launched: November 2012

B Stakeholders who are party to the agreement: Governments of SADC

C. Total number of signatories/supporters of the agreement: N/A

D. Organization responsible for ongoing management of the agreement: International Telecommunication Union (ITU) and the European Commission through HIPSSA project

C. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

    "A person who intentionally, without lawful excuse or justificationor in excess of a lawful excuse or justificationhinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both"

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools**. N/A
4. **Recognizing computer emergency response teams as a protected and benign group**. N/A
5. **Recognizing human rights online and/or right to privacy**. N/A
6. **Cooperation with states to increase stability and security in use of ICTs.** N/A
7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure**. N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** N/A

F. Additional norms included in the agreement:

It does not address norms but more specific to offences thus indirectly addressing norms such as harmful use of ICT's, criminalising hate speech and denial of genocide and crimes against humanity.

XVI. Paris Call for Trust and Security in Cyberspace.

A. Date it was signed/launched: November, 2018

B. Stakeholders who are party to the agreement: Multistakeholder – governments, industry, civil society, academia, public sector

C. Total number of signatories/supporters of the agreement: 1105

D. Organization responsible for the agreement: French Ministry of European and Foreign Affairs

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

    ***Protect individuals and infrastructure** – Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.*

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools**. Yes.
    a. ***Lifecycle security** – Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.*
    b. ***Non-proliferation** – Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.*
4. **Recognizing computer emergency response teams as a protected and benign group**. N/A

5. **Recognizing human rights online and/or right to privacy.** Yes.

    In order to respect people's rights and protect them online as they do in the physical world, States must work together, but also collaborate with private-sector partners, the world of research and civil society.

6. **Cooperation with states to increase stability and security in use of ICTs**. Yes.

    ***Supporters of the Paris Call [including states] are therefore committed to working together to: [list all nine principles*]**

7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure.** Yes.

    ***Protect individuals and infrastructure** – Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.*

10. States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.

    ***Protect individuals and infrastructure** – Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.*

11. Encourage responsible reporting of ICT vulnerabilities and share remedies – **Yes.**

    ***Non-proliferation** – Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.*

F. Additional norms included in the agreement:

- **Protect the Internet** – Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.
- **Defend electoral processes** – Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.
- **Defend intellectual property** – Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector.
- **Cyber hygiene** – Support efforts to strengthen an advanced cyber hygiene for all actors.
- **No private hack back** – Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.
- **International norms** – Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

XVII. Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

A. Date it was signed/launched: July 2015

B. Stakeholders who are party to the agreement: UN Member States by General Assembly resolution adopting the report.

C. Total number of signatories/supporters of the agreement: 193

D. Organization responsible for ongoing management of the agreement: N/A

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

Note: This is the agreement which established all the of the GGE norms. They are all reflected.

1. **States should not allow territory be used for international wrongful acts via ICTs**. Yes.

   "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;"

2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

   "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;"

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** Yes.

   "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"

4. **Recognizing computer emergency response teams as a protected and benign group**. Yes.

   "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."

5. **Recognizing human rights online and/or right to privacy.** Yes.

   "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13on 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;"

6. **Cooperation with states to increase stability and security in use of ICTs**. Yes.

   "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;"

7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** Yes.

   "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;"

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes.

   "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;"

9. **States (or other stakeholders) should protect their own critical infrastructure.** Yes.

   "*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;"*

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** Yes.

    "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."

11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** Yes.

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

F. Additional norms included in the agreement:

Confidence Building Measures

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.

International Cooperation

The 2013 report called upon the international community to work together in providing assistance to: improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use.

International Law

The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.

XVIII. Siemens' Charter of Trust

A. Date it was signed/launched: March, 2018

B. Stakeholders who are party to the agreement: Multistakeholder

C. Total number of signatories/supporters of the agreement: 13

D. Organization responsible for ongoing management of the agreement: Charter of Trust Secretariat

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** Yes.

   "(2) Responsibility throughout the digital supply chain

   Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them."

4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy**. N/A
6. **Cooperation with states to increase stability and security in use of ICTs.**

   "(5).Innovation and co-creation

   Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.a. contractual Public Private Partnerships"

"(10) Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay."

7. **States (or other stakeholders) should consider all relevant information following ICT incidents**. N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes.

   "(8)Transparency and response

   Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice which is focusing on critical infrastructure."

9. **States (or other stakeholders) should protect their own critical infrastructure.** Yes.

   "(7.) Certification for critical infrastructure and solutions

   Companies – and if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions."

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** N/A

F. Additional norms included in the agreement:

1.Ownership for cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "It is everyone's task".

2.Responsibility throughout the digital supply chain

Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate. Continuous protection: Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

3.Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

4.User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer's cybersecurity needs, impacts, and risks.

6.Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future.

9.Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).

XIX. Global Commission on the Stability of Cyberspace’s Six Critical Norms

A. Date it was signed/launched: November, 2019

B. Stakeholders who are party to the agreement: Government, Industry, Civil Society

C. Total number of signatories/supporters of the agreement: 10

D. Organization responsible for ongoing management of the agreement: Commission on the Stability of Cyberspace (GCSC)

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** Yes.

   State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** Yes.
   - *NORM to Avoid Tampering: State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace*
   - *NORM Against commandeering of ICT Devices into botnets: State and non-state actors should not commandeer the general public’s ICT resources for use as botnets or for similar purposes.*
4. **Recognizing computer emergency response teams as a protected and benign group.** N/A
5. **Recognizing human rights online and/or right to privacy.** Yes.

   Not being listed in these 8 norms but listed in the principles: Respect for Human Rights: Efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

6. **Cooperation with states to increase stability and security in use of ICTs.** Yes.
7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** Yes.

   Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** Yes.

   States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

9. **States (or other stakeholders) should protect their own critical infrastructure**. Yes.

   Protecting Electoral infrastructure: State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**. Yes.

    (Same as item 8.) States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

F. Additional norms included in the agreement:

1) State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

2) State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

3) States should enact appropriate measures, including laws, regulations, and training and capacity building, to ensure basic cyber hygiene.

4) Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

XX. Commonwealth Cyber Declaration

A. Date it was signed/launched: 16-20 April, 2018

B. Stakeholders who are party to the agreement: Governments in the Commonwealth of Nations

C. Total number of signatories/supporters of the agreement: 54 countries

D. Organization responsible for ongoing management of the agreement: Commonwealth Secretariat

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure**. N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** Yes**.**

   Not listed in the declaration, but they listed these below:

   Highlight the importance of national cybersecurity strategic planning and establishing incident response capabilities, supported by appropriate legislation and a law enforcement and criminal justice system capable of addressing cybercrime.

5. **Recognizing human rights online and/or right to privacy.** Yes.

   Not specific about privacy, but identified human rights:

   a) Affirm that the same rights that citizens have offline must also be protected online.

   b) Recognise that access to information and digital literacy can be a powerful catalyst for economic empowerment and inclusion, and commit to take steps towards expanding digital access and digital inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language.

   c) *Emphasise that enhanced digital inclusion of young people in the Commonwealth can contribute in a positive way to their education, social engagement and entrepreneurship*.

6. **Cooperation with states to increase stability and security in use of ICTs.** Yes.

   Commit to promote frameworks for cyberspace, including the applicability of international law, agreed voluntary norms of responsible state behavior, and the development and implementation of confidence building measures to encourage trust, cooperation and transparency, consistent with the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International security (UNGGE).

7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A

9. **States (or other stakeholders) should protect their own critical infrastructure.** Yes.

   Recognising the threats to stability in cyberspace and integrity of the critical infrastructure and affirming our shared commitment to fully abide by the principles and purposes of the Charter of the United Nations to mitigate these risks;

10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** Yes.

    Commit to use national contact points and other practical measures to enable cross-border access to digital evidence through mutually agreed channels to improve international cooperation to tackle cybercrime

11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** Yes.

    Commit to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures.

F. Additional norms included in the agreement:

- *Commit to promote interoperable and global technical standards, through appropriate consultative processes involving industry, academia, governments and other relevant stakeholders, recognising that standards should be open, foster security and trust and not act as barriers to trade, competition or innovation.*
- *Highlight the importance of common standards and the strengthening of data protection and security frameworks, in order to promote public trust in the internet, confidence for trade and commerce, and the free flow of data*
- *Acknowledge the importance of tolerance, respect for diversity, and understanding in cyberspace.*
- *Affirm that the same rights that citizens have offline must also be protected online*.

XXI. A Contract for the Web

A. Date it was signed/launched: November, 2019

B. Stakeholders who are party to the agreement: Multistakeholder

C. Total number of signatories/supporters of the agreement: Over 1,000, including individuals

D. Is there an organization responsible for ongoing management of the agreement: World Wide Web Foundation

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs**. N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure**. N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.**
5. **Recognizing human rights online and/or right to privacy.** Yes.

   Principle 3: Respect and protect people's fundamental online privacy and data rights

6. **Cooperation with states to increase stability and security in use of ICTs.**

   [From preamble] "*To achieve the Contract's goals, governments, companies, civil society and individuals must commit to sustained policy development, advocacy, and implementation of the Contract text.*"

7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** N/A
8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs.** N/A
9. **States (or other stakeholders) should protect their own critical infrastructure.** N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack.** N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies**. Yes.

Principle 6-1(c) – “*By being accountable for their work, through regular reports, including how they are… c. Assessing and addressing risks created by their technologies…”*

F. Additional norms included in the agreement:

Governments will…

1. Ensure everyone can connect to the internet
2. Keep all of the internet available, all of the time
3. Respect and protect people’s fundamental online privacy and data rights

Companies will…

1. Make the internet affordable and accessible to everyone
2. Respect and protect people’s privacy and personal data to build online trust
3. Develop technologies that support the best in humanity and challenge the worst

Citizens will…

1. Be creators and collaborators on the Web
2. Build strong communities that respect civil discourse and human dignity
3. Fight for the Web

XXII. EthicsfIRST

A. Date it was signed/launched: Information not available

B. Stakeholders who are party to the agreement: EthicsfIRST is designed to inspire and guide the ethical conduct of all Team members, including current and potential practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way.

C. Total number of signatories/supporters of the agreement : Information not available

D. Organization responsible for the agreement: First, Improving security Together

E. Are any of the following norms included in the agreement (adapted from 2015 UN-GGE consensus report)?

1. **States should not allow territory be used for international wrongful acts via ICTs.** N/A
2. **Do not conduct or support ICT activity that harms critical infrastructure.** N/A
3. **Protections for ICT supply chain security, preventing the spread of malicious ICT tools.** N/A
4. **Recognizing computer emergency response teams as a protected and benign group.** Yes.

   Duty to Team health

   Teams have a responsibility to continue to provide the services they have promised their constituents. This responsibility includes the physical and emotional health of the Team.

   In order to both respect as individuals the members who make up a Team and enable the longterm viability of sustaining an adequate level of service, a Team should strive to maintain a healthy, safe, and positive work environment that supports the physical and emotional health of (all) its members. In order to respond to a crisis, "normal" operations should support emotional health and stress reduction.

5. **Recognizing human rights online and/or right to privacy.** Yes.

   “Duty to respect human rights

   Team members should be aware that their actions may impact human rights of others through the sharing of information, a possible bias in their actions, or an infringement of property rights. Team members have access to a wide *range of personal, sensitive, and confidential information in the course of handling incidents. This information should be handled in a way to uphold human rights.*

During incident handling, responders should not act in a biased manner and should do their utmost to eliminate bias from their processes and decision-making, either performed by responders or built into algorithms.

For the purpose of this principle, the notion of "property" (UN Declaration of Human Rights: Article 17) includes intangibles such as intellectual property, as well as ideas and concepts in general, regardless of whether they are legally protected (e.g., patented)."

6. **Cooperation with states to increase stability and security in use of ICTs.** N/A
7. **States (or other stakeholders) should consider all relevant information following ICT incidents.** Yes.

   Duty of coordinated vulnerability disclosure

   Team members who learn of a vulnerability should follow coordinated vulnerability disclosure by cooperating with stakeholders to remediate the security vulnerability and minimize harm associated with disclosure. Stakeholders include but are not limited to the vulnerability reporter, affected vendor(s), coordinators, defenders, and downstream customers, partners, and users.

   Data that may help other response Teams in their efforts related to other incidents should be made available to them, possibly in redacted form. Information that is confidential and proprietary should only be made available with appropriate protections.

8. **States (or other stakeholders) should work to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs**. Yes.

   Team members should coordinate with appropriate stakeholders to agree upon clear timelines and expectations for the release of information, providing enough details to allow users to evaluate their risk and take actionable defensive measures.

9. **States (or other stakeholders) should protect their own critical infrastructure.** N/A
10. **States (or other stakeholders) should respond when asked for help by other states whose critical infrastructure is harmed by cyberattack**. N/A
11. **Encourage responsible reporting of ICT vulnerabilities and share remedies.** Yes.

    Duty to inform

    Team members should consider it their duty to keep their constituents informed about current security threats and risks. When Team members have information that can either adversely affect or improve safety and security, they have a duty to inform relevant parties or others who can help, with appropriate effort, while duly considering confidentiality, privacy laws and regulations, and other obligations.

F. Additional norms included in the agreement:

- IETF RFC2119 for the definition of "SHOULD
- UN Declaration of Human Rights: Article 17

Annex – Links and resources

BPF Cybersecurity session at IGF 2020
Tuesday, 17 November 2020 (virtual meeting)

Agenda and report
https://www.intgovforum.org/multilingual/content/igf-2020-bpf-cybersecurity
Recording
https://youtu.be/zxqh4Em7twg

BPF draft reports (published September 2020)

Background paper – What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance
https://www.intgovforum.org/multilingual/filedepot_download/10387/2252

Research paper – Exploring Best Practices in Relation to International Cybersecurity Agreements
https://www.intgovforum.org/multilingual/filedepot_download/10387/2253

Input received in response to the BPF's Call for Contributions

Australian Strategic Policy Institute ASPI
https://www.intgovforum.org/multilingual/filedepot_download/10387/2329

Duncan Hollis
https://www.intgovforum.org/multilingual/filedepot_download/10387/2301

EastWest Institute
https://www.intgovforum.org/multilingual/filedepot_download/10387/2300

Global Commission on the Stability of Cyberspace GCSC
https://www.intgovforum.org/multilingual/filedepot_download/10387/2298

Tim Maurer
https://www.intgovforum.org/multilingual/filedepot_download/10387/2302

Outline proposal for a BPF on Cybersecurity in 2020
https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9615/1913