IGF 2020

Best Practice Forum on Cybersecurity

What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance

Background paper

September 2020

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 <mknodel@cdt.org>;
Authors: Apratim Vidyarthi and Anastasiya Kazakova;
Contributors: Maarten Van Horenbeeck and Sheetal Kumar;
Copy: Wim Degezelle.

www.intgovforum.org/multilingual/content/bpf-cybersecurity

Table of contents

Introduction

The *Internet Governance Forum (IGF)* is a global forum, convened by the United Nations Secretary General[1] where governments, civil society, the technical community, academia, the private sector, and independent experts discuss Internet governance and policy issues.[2]

The IGF *Best Practice Forums (BPF)* provide a platform 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 multilateral -- 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 are referenced.

Looking ahead to the 2020 intersessional report, members of the BPF reflect 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[3] 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

[1] The resolution adopted by the UN General Assembly on 16 December 2015, (70/125) 'Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society', extended the mandate of the IGF as set out in paragraphs 72 to 78 of the Tunis Agenda.
[2] IGF website: http://www.intgovforum.org - the IGF is one of the key outcomes of the World Summit for the Information Society (WSIS).
[3] https://www.un.org/disarmament/open-ended-working-group/

perspectives that went beyond those 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 or 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 as a result 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 they 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 to this, the BPF on Cybersecurity concluded in 2019 that different norm initiatives are filling gaps where more binding policy measures are not possible because there is a lack of a collective understanding of what the issues are and no agreement among stakeholders on adequate mitigations. However, there are the beginnings of consensus expectations that, across different initiatives, can become a common basis to build on. Furthering these processes will best focus on identifying common goals and then fulfillment of those goals with the requisite creativity that only multistakeholder and multidisciplinary collaboration can bring.

Analysing Cybersecurity Agreements

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

Cybersecurity agreements were initially scoped in agreements based on three high level 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 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).

It was determined that the agreements analysed typically have four horizontal components:

1. Foundational principles, which guide development of norms or agreement. These may be for instance, 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 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 key elements were identified:

- Further multi-stakeholderism: identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.
- Responsible disclosure: the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
- Reference to International Law: whether the agreement mentions the importance of international law, or commits the signatories' behavior to international law.
- Definition of Cyber threats: whether the agreement proposes a clear or aligned definition of cyber threats.
- Definition of Cyber-attacks: whether the agreement proposes a clear or aligned definition of cyber attacks.
- Reference to Capacity Building: whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.
- Specified CBMs: whether the agreement describes or recommends specific Confidence Building Measures.
- Reference to Human Rights: whether the agreement reflects on the importance of human rights online.
- References to content restrictions: whether the agreement discusses the need for content restrictions online.

- Vulnerability equities processes: the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes 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 or make no impact. 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 to understand the most optimal way, given the particular context, to make norms work. This learning process includes recognizing possible blind spots, 'closed doors' and, on the contrary, opportunities, 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. There are certain ingredients to consider.[4] To facilitate norm development, a number of factors should be considered – we analyze them in detail in the following section. Practical experience, however, shows that while it is important to have influential powerful norm promoters, incentives for others to support norm development are not always sufficient and this can lead to a 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 some significant world events can foster the norm development process. However, since "we are in the relative infancy of thinking about this issue"[5] and it is yet to define rules of the game in cyberspace and draw lines[6], states can easily alter their positions, opinions and attitudes if doing so serves their interests. And this complicates norm development and may lead to frustration – or, vice versa, make norms emerge and work. The lesson here is that it is necessary to keep this in mind and be prepared: we cannot exactly predict or control the entire norm development process as there are many factors to consider and they can be

[4] M. Finnemore & D.H.Hollis "Constructing norms for global cybersecurity" https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf

[5] Chris Painter, formed US Cyber diplomat,quoted in https://foreignpolicy.com/2015/05/13/the-state-departments-weary-soldier-in-americas-cyber-war-christopher-painter/

[6] This is also proved by the fact that many states are only at the very beginning of the process to develop regulations, laws and processes for cyberspace.

beyond our capacities. But even failures teach and create opportunities for further successful efforts.

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 can 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[7] enhancing security and stability in cyberspace – without necessarily leading to public contestation of norms.

[7] For instance, capacity building efforts might trigger 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

So while the implementation and operationalisation of cybernorms remains a challenge for all actors, the premise of this report is that understanding how norms can be better adopted and operationalised would benefit from an analysis of 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, it is hoped that 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."[8] 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 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,"[9] which encompasses both implicit and explicit norms. Within this broad definition, norms should be concrete and specific.[10] In contrast to implicit norms, the strongest category of explicit norms are defined in international law through the principles of *jus cogens*, which centers around norms that are accepted and recognized by nation states and from which "no derogation is permitted."[11] *Jus cogens* principles commonly apply to customary international law, treaty provisions, and general principles of norms.[12] *Jus cogens* requires evidence - such as public statements, legal opinions, laws, and legal decisions - showing that these norms have

[8] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).
[9] Geoffrey Vickers, *Values, Norms, and Policies*, 4 Policy Sciences 103, 103 (1973).
[10] *Id*. at 104.
[11] International Law Commission, *Report on the work of the seventy-first session chapter V: Peremptory norms of general international law (*jus cogens*)*, ℙ56, Part One, Conclusion 2, U.N. Doc. A/74/10 (2019) (https://legal.un.org/ilc/reports/2019/english/chp5.pdf).
[12] *Id*. at ℙ56, Part One, Conclusion 5.

been accepted and recognized,[13] and that a large majority of states accept these norms.[14] Under *jus cogens*, some norms form the bedrock of international law and are "so fundamental as to be nonderogable under any circumstances."[15] 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.[16] 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.[17]

This basic overview of international law reveals the existence of a hierarchy of explicit norms.[18] 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 (who to govern?), behavior (what does 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.

More details on the framework for our analysis of norm development are below.

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.[19] This reflects a normative life cycle: generally, norms emerge through social processes, often propagated by politically engaged entities.[20] Second, the norm is adopted, normally through transnational organizations socializing these norms.[21] 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.[22] Within this life

[13] *Id*. at ℙ56, Part One, Conclusion 6.
[14] 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)
[15] *Id*. at 308.
[16] *Id*. at 335.
[17] *Id*. at 340, 342.
[18] *Id*. at 339.
[19] Knut Traisbach, *International Law*, E-International Relations (Jan. 1, 2017), (https://www.e-ir.info/2017/01/01/international-law/)
[20] Id.
[21] Id.
[22] Id.

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 barrier 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 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*.[23] Thus, to get from acceptable norms to fundamental or *jus cogens* norms requires legal obligation in practice. With regard to cyberspace, we could generally observe norms promotion and norms enforcements 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.[24]

The examples of sources for norm-setting and norm development could be grouped into three types depending on the source of the norm:

- Multilateral norm diplomacy and state-driven efforts: joint statements (e.g. on advancing responsible state behavior[25], on 'Infodemic'[26]); joint proposals (e.g. malicious cyber activity against healthcare services[27]); exchange of views between states (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[28]); state-led and state-initiated processes (e.g. dialogues[29], Global Commission on the Security of Cyberspace[30], Paris Call for Trust and Security in Cyberspace[31]) with participation of non-state actors; 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[32]); publishing of compilation of norm implementation guidance (e.g. Australian compilation[33]).

---

[23] 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)
[24] The 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 Chian's malicious cyber-activity.
[25] https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/
[26] https://unny.mission.gov.au/files/unny/120620%20Cross-Regional%20Statement%20on%20Infodemic%20in%20the%20Context%20of%20COVID-19.pdf
[27] https://front.un-arm.org/wp-content/uploads/2020/05/final-joint-oewg-proposal-protection-of-health-infrastructure.pdf
[28] https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf
[29] https://genevadialogue.ch/
[30] https://cyberstability.org/
[31] https://pariscall.international/en/
[32] 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
[33] https://www.dfat.gov.au/sites/default/files/compilation-norm-implementation-guidance.pdf

- Subject-matter, expert-driven and civil society efforts: analyzing norm definition and norm operationalization (e.g. The Hague Program for Cyber Norms[34] and Global Partners Digital's work on analysing norms[35]); 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[36], ICRC's call to global leaders to stop cyberattacks on healthcare sector[37]).

- Industry-led process: establishing calls to governments to agree on certain norms of behavior (e.g. Digital Geneva Convention[38], Manifesto for a New Digital Deal[39], CyberPeace Institute's call to governments to stop attacks on healthcare[40]); establishing industry organizations based on participants' consensus around particular norms of behavior (e.g. Charter of Trust[41], Tech Accord[42]); establishing initiatives for norm operationalization, including developing of confidence building and capacity building efforts (e.g. Global Transparency Initiative[43]).

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).[44] Unilateral policy changes -

---

[34] https://www.thehaguecybernorms.nl/
[35]https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-cyber-norms/
[36]https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea
[37] https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/
[38] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/
[39] https://www.telefonica.com/digital-manifesto/
[40] https://cyberpeaceinstitute.org/campaign/call-for-government
[41] https://www.charteroftrust.com/
[42] https://cybertechaccord.org/accord/
[43] https://www.kaspersky.com/transparency-center
[44] Peters 2017.

especially in the context of the internet - are less relevant to norm implementation, given that norms require widespread acceptance and multistate codification and signature.[45]

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 frameworks and conventions which implement soft law.[46] 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, the former internalizing the norms, while the latter gathers 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.

[45] *Infra* Defining Norms (p. 3).
[46] 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)

Analysis framework: 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.

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.[47] 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, choosing and framing the context for norm development seems essential. Framing the context for defining norms is not always easy to do and requires much 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 identified in norms should also be linked to larger issues to be easily understood to 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 would create 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 (NGOs) (e.g. Transparency International), private sector entities (e.g. Microsoft, Charter of Trust), international organizations (e.g. the EU, UN). Powerful, influential and widely respected leaders

[47] Finnemore and Hollis "Constructing Norms for Global Cybersecurity" 2016https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf

and/or a 'high-ambition coalition'[48] of states can be crucial for norm emergence and for encouraging others to give support. 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.** 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?' (*identity*). Norms are created to address particular problems and should be specific in communicating specific actions that need to be taken (*behavior*) – 'what does the norm say?'. 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. Finally, 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.** As mentioned above, norms are not static products, but rather 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, of which there are three – incentives, persuasion, and socialization – and it is up to norm entrepreneurs to maneuver and decide which tool fits the context better. For instance, it can be important to align *incentives* with state behavior – if incentives are not provided, states would not be motivated to adopt norms. Incentives are applied when norm entrepreneurs create political attractiveness and value for specific actors – for instance, by telling [NH1] about 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',[49] 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. *Persuasion* can be coupled with incentives, and as a message 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

[48] https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf
[49] Claude 1966 https://www.jstor.org/stable/2705629

behavior and adhere to the norm. Finally, *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 as well as 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 is the first trap 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.[50] Multi-stakeholder 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, multi-stakeholder engagements comprised of actors with backgrounds, values, interests[51] and incentives that are too different might also make negotiations more complicated in trying to achieve particular results, as well as make stakeholders less open to candidly discuss issues.[52] This is the second trap leading to failure and highlighting that starting with a small group of actors that share the same values even though they represent different stakeholder groups would on the contrary be more willing to 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

[50] Hollis and Finnemore 2016 https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf
[51] Interests could be indeed different, but still overlap and support each other.
[52] Id.

persuasion.[53] The absence of a 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, it should be complemented with incentives, i.e., the promised reward needs to be greater than the cost of fulfilling the conditions of the reward.

Lack of incentives for internalizing norms[56] might be 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 can not only positively impact norm-setting and sometimes even be a crucial factor in defining a norm, it may also break norms if it is in the interest of powerful leaders and if benefits outweigh the cost of not adhering to norms. And this is particularly common in cases where there is a lack of enforcement powers, or 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 lack 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 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.

---

[53] Halliday at 1170.
[54] Panke at 732.
[55] Id. at 1174.
[56] https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf
[57] Axelrod 1986 "An Evolutionary Approach to Norms", 1105
[58] Id. at 730.
[59] Panke at 732.

Domestic legal institutions and domestic powers can also play a critical role in a state's non-compliance with a norm. Quite often the actual decision of whether or not to adhere to or violate a norm 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[60] the interests of domestic powers (if these powers do not support norm adherence). Therefore, 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, different scenarios could be applied:

- **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 to create legitimacy and reduce effort and startup costs for norm entrepreneurs, and thus make 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).

- **Favoring fragmentation and cross-pollination of cyber norms efforts**[65] **together with promoting muli-stakeholder engagements.** Fragmentation can help address

---

[60] Diana Panke & Ulrich Petersohn, *Why International Norms Disappear Sometimes*, 18 Eur. J. Int. Relations 719, 725 (2012) (https://www.researchgate.net/publication/258135219)
[61] https://undocs.org/A/70/174
[62] https://www.first.org/global/sigs/ethics/ethics-first
[63]https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/05/15091233/RVD-Ethical-Principles-EN.pdf
[64]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
[65] https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf

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. Multi-stakeholder 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' [68] for the actions of a small governing minority. 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.

[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] https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf p.12

Case studies: Analyzing Successful Global Norms

Using the norms test defined in Section II, we can 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

[69] Lawrence Freedman, *Disarmament and Other Nuclear Norms*, 36 Washington 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).

these nuclear norms, including sanctions and an embargo on access to nuclear technologies, has forced the continued existence of these norms, 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 lies in/is 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

[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.

hostages who may on a basis of reciprocity suffer if it violates the rules of diplomatic immunity, or may be 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" (https://legal.un.org/avl/ha/vcdr/vcdr.html)

"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."
https://www.britannica.com/topic/diplomatic-immunity

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.[74] These principles led to the development of Global Sullivan Principles (GSP), which advance human rights and social justice internationally.[75] 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,the Gap, and Levi Strauss.[76] While the original Sullivan Principles have mixed reviews and were considered as not going far enough,[77] many companies signed on to the principles, and these companies did better on the stock market than stock averages.[78] Additionally, the original Sullivan Principles encouraged companies to withdraw from South Africa when the principles were violated or unimplementable.[79]

Within the four factors for norms, the newer GSP (coming into effect in 1999) lack specificity or metrics against which to measure accomplishment.[80] 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 -

[74] Steven R. Ratner, *International Law: The Trials of Global Norms*, 110 Foreign Policy 65, 72 (1998) (http://www.jstor.com/stable/1149277).
[75] The Global Sullivan Principles, University of Minnesota Human Rights Library, http://hrlibrary.umn.edu/links/sullivanprinciples.html (last accessed July 1, 2020).
[76] Ratner, *supra* note 76, at 72.
[77] 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).
[78] Malek K. Lashgari & David R. Grant, *Social Investing: The Sullivan Principles*, 47 Rev. Social Econ. 74, 80 (1989).
[79] Mzamo P. Mangaliso, *South Africa: Corporate Social Responsibility and the Sullivan Principles*, 28 J. Black Stud. 219, 229 (1997).
[80] Gwendolyn Yvonne Alexis, Green Business: An A-to-Z Guide, (Nevin Cohen Ed., 2010).

given the lack of enforcement mechanisms, outside of the opportunity cost of signing on to them and receiving positive recognition for doing so.[81] 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.[82] 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.[83] 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.[84] These Guidelines are a soft law that acts as a standard for global regulations.[85] The guidelines are not binding, but influence new laws and treaties by promoting the movement of capital internationally.[86] They are also a model for national laws.[87]

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.[88]

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

---

[81] Geral F. Cavanagh, *Global Business Ethics: Regulation, Code, or Self-Restraint*, 14 Bus. Ethics Q. 652, 638 (2004).
[82] *Id.* at 633.
[83] *Id*.
[84] Steven R. Ratner, *International Law: The Trials of Global Norms*, 110 Foreign Policy 65, 68 (1998) (http://www.jstor.com/stable/1149277).
[85] *Id*.
[86] 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).
[87] *Id*.
[88] *Id.*

promoting stability in cyberspace. As these two processes continue 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[89], 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-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

[89] Full report of the BPF Cybersecurity
https://www.intgovforum.org/multilingual/filedepot_download/8395/1896

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.

Feedback on this report

We value your feedback on this report !

Feel free to reach out the report's Editor, Mallory Knodel <mknodel@cdt.org>, with comments and questions.

Substantive feedback can be submitted via the BPF's Call for Contributions
https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2020-call-for-contributions

Introducing the BPF Cybersecurity 2020 report

This paper made up one of three workstreams in the 2020 Best Practices Forum on Cybersecurity. This year, the group is focusing on:

1. Revisiting the list of cybersecurity agreements the BPF identified in 2019, and evaluate whether new agreements were developed since then which have taken on a significant normative role;
2. Bringing in expertise from other normative domains, and evaluating whether these can be applied to cybersecurity;
3. Widen the participation in the BPF, through awareness building and increasing the diversity of participants in the Best Practices Forum.

Bringing these three areas of work together, the BPF intends to make a meaningful, multi-stakeholder contribution to the domain of cyber norms. This paper is the contribution from the second workstream of this year's BPF, contributing findings from several case studies of normative behaviors.

Please check the BPF Cybersecurity webpage for details on the other workstreams, the BPF Cybersecurity session[90] during the virtual IGF 2020, and the BPF 2020 output report:
https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

[90] The session is currently planned for Tuesday 17th November, 12:50-14:20 UTC.
Check the IGF2020 schedule for updates:
https://www.intgovforum.org/multilingual/content/igf-2020-schedule-0