IGF 2018
Best Practice Forum on Cybersecurity

IGF2018 Best Practice Forum on Cybersecurity:

Cybersecurity Culture, Norms and Values

December 2018

Disclaimer:
The IGF Secretariat has the honour to transmit the paper prepared by the 2018 Best Practice Forum on Cybersecurity. The content of the paper and the views expressed therein reflect the BPF discussions and are based on the various contributions received and do not imply any expression of opinion on the part of the United Nations.

Table of contents

Executive summary & Key learnings

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. The outputs from this programme are intended to become robust resources, to serve as inputs into other pertinent forums, and to evolve and grow over time. BPFs offer substantive ways for the IGF community to produce more concrete outcomes.

Since 2014, the IGF has operated a Best Practice Forum focused on cybersecurity. In 2014-2015, the BPF worked on identifying Best Practices in Regulation and Mitigation of Unsolicited Communications and Establishing Incident Response Teams for Internet Security. Later, the BPF has been focused on cybersecurity; identifying roles and responsibilities and ongoing challenges in 2016, and identifying policy best practices in 2017.

For 2018, the Best Practices Forum focused its work on the culture, norms and values in cybersecurity. The plan of action we took to approach this topic consisted of:

- The BPF started the process by building on its previous work on the roles and responsibilities of the IGF stakeholder groups in cyberspace and explore what norms have developed that apply to each of these groups. Some of the questions we explored relate to the behaviour of each stakeholder group, such as "state behaviour" or "industry behaviour". The discussion of civil society's role in norms development includes social norms of safe and secure online behaviour by individual users.

- We identified sample norms established by various forums, documenting and comparing them. We did so by engaging experts, BPF contributors and the IGF's network of National and Regional IGF initiatives (NRIs). Through this network, BPFs can bring in a developing country perspective and connect the NRIs with the norms development communities, to promote a culture of cybersecurity. We collected information on how they are articulated, implemented and whether they are successful.

- The BPF leveraged the work from last year to identify if any of the policy recommendations may see widespread acceptance, and may have developed into a recognized "best practice".

- We aimed to understand the impact of a "digital security divide". When or where there's no real universal implementation of a norm, or if the implementation of the norm has unintended consequences, or has different impacts in a different context (e.g. those with and those without effective rule of law), it may result in a group of "haves" and "have nots" in terms of the protection the norms offer. Security controls will be sufficient or meaningful in some parts of the world, and not in others. While these differences may exist regardless of norms, inappropriate norms implementation

also may adversely affect users. This is an interesting area for investigation into the reasons for non-adherence or potential barriers preventing the implementation.

- Finally, we convened a meeting during the Paris IGF, bringing in experts from the norms development community to discuss the key issues in this space.

At the beginning of the year, we published a Background document that was developed with support from participants in the Best Practice Forum, and serves as an introduction to the wider area. It was provided as background reading to anyone responding to our public Call for Input, which was released on August 15th.

The document you are reading today brings together the research performed by the BPF, the inputs from 16 contributors to our call for input, and the contributions by experts and participants in our Paris session on November 14th. Key lessons learned in our work include:

- **The importance of norms** as a mechanism in cybersecurity for state and non-state actors to agree on a responsible way to behave in cyberspace, given that the speed of legislation often struggles to keep up with the pace of changes in the sphere of cybersecurity. In addition to the development of norms, it is important that **stakeholders continue to focus on mechanisms for norms implementation**, to ensure their effectiveness.

- **The importance of multi-stakeholderism** – threats to cybersecurity impact governments, private companies and people. There are a number of helpful norms, on different aspects and from various parts of the world, but more needs to be done to involve non-state stakeholders in the development and implementation of norms. It should also be noted that there are several norms developed and proposed by non-state actors, which do not always get the same level of attention.

- **Cybersecurity norms and laws should be respectful of human rights**, and not stray into areas such as freedom of expression and control of content online. It is important to separate the security of the infrastructure, which this BPF is focused on, from questions of content shared online.

We hope this information proves useful to develop the community's understanding of the complex but important area of cyber norms development, and how we all partner on building a culture of cybersecurity that protects and enables society online.

Introduction to the Best Practices Forum on Cybersecurity

Introduction

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.[1] The outputs[2] from this programme are intended to become robust resources, to serve as inputs into other pertinent forums, and to evolve and grow over time. BPFs offer substantive ways for the IGF community to produce more concrete outcomes.

Since 2014, the IGF has operated Best Practices Forums on topics related to cybersecurity. In 2014-2015, BPFs worked on identifying Best Practices in Regulation and Mitigation of Unsolicited Communications and on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security. In 2016 the BPF Cybersecurity studied how enhanced collaboration and collaboration between stakeholders can contribute to building confidence and security in the use of ICTs and in 2017 the BPF focussed on cybersecurity policy best practices and development.

As part of its work in 2017 the BPF consulted with the community on what areas would benefit from further stakeholder conversation and a possible way forward for the BPF. Two areas surfaced '*Defining and identifying a cybersecurity culture, norms and values,'* and '*Identifying the risk of a potential digital security divide, between those who have and those who do not have access to cybersecurity measures'.* This lead to the formulation of the proposal[3] for a BPF on cybersecurity in 2018, which was confirmed by the IGF Multistakeholder Advisory Committee (MAG).

For 2018, the Best Practices Forum is focusing on the culture, norms and values in cybersecurity.

- The BPF is starting the process by building on its previous work on the roles and responsibilities of the IGF stakeholder groups in cyberspace and explore what norms have developed that apply to each of these groups. Some of the questions relate to the behaviour of each stakeholder group, such as "state behaviour" or "industry behaviour". The discussion of civil society's role in norms development includes social norms of safe and secure online behaviour by individual users.
- Further work will identify norms established by various forums, documenting and comparing them. Of particular value would be the IGF's network of National and

[1] The BPF intends to enrich the IGF output *'to enhance the impact of the IGF on global Internet governance and policy'*as called for in the report by the UN General Assembly Economic and Social Council (ECOSOC) Working Group on Improvements to the IGF (March 2012).
[2] BPF archived content 2014-2017: https://www.intgovforum.org/multilingual/content/bpfs-archived-content.
[3] MAG Proposal for a BPF on Cybersecurity in 2018: http://www.intgovforum.org/multilingual/filedepot_download/6119/1181

Regional IGF initiatives (NRIs). Through this network, the BPF can bring in a developing country perspective and connect the NRIs with the norms development communities, to promote a culture of cybersecurity. Part of this process would be to make sure that their norms are well known and understood, and to provide a space for discussion. We'll collect information on how they are articulated, implemented and whether they are successful.

- The BPF will also leverage the work from last year to identify if any of the policy recommendations may see widespread acceptance, and may have developed into a recognized "best practice". This could then lead to other norms development bodies considering them as new norms - consistent with one of the IGF's purposes to bring emerging issues to the attention of the relevant bodies.
- The focus on culture, norms and values will lead us down the path of understanding the impact of a "digital security divide". When or where there's no real universal implementation of a norm, or if the implementation of the norm has unintended consequences, or has different impacts in a different context (e.g. those with and those without effective rule of law), it may result in a group of "haves" and "have nots" in terms of the protection the norms offer. Security controls will be sufficient or meaningful in some parts of the world, and not in others. While these differences may exist regardless of norms, inappropriate norms implementation also may adversely affect users. This is an interesting area for investigation into the reasons for non-adherence or potential barriers preventing the implementation.

Structure of the document

This report is structured in two parts. The first part (part I) provides an introduction to cybersecurity culture, norms and values. It explores different concepts and definitions, looks at how norms are developed, and zooms in on venues for the development of cybersecurity norms and their implementation. It serves as a background reading and helps to identify where gaps exist.

The second part of the report summarizes the input the BPF received on its Call for contributions that was launched on 15 August 2018, an as part of which the community was asked to provide answers on 7 open questions related to the definition of cybersecurity, relevant norms and values, norms promoters, examples of successful and less successful norms, methods for implementing cybersecurity norms, and the existence of a Digital Security Divide. The BPF received 16 contributions.

Acknowledgements

This BPF output document is the result of a collaborative effort of many.
We would like to recognise the MAG for selecting cybersecurity as topic for a BPF as part of the 2018 intersessional work program; the BPF Co-Facilitators Mr. Markus Kummer and Mr.

Ben Wallis and the BPF Lead-Expert Mr. Maarten Van Horenbeeck for their guidance and leadership; BPF Consultant Mr. Wim Degezelle supporting the BPF on behalf of the IGF Secretariat; the key contributors to the BPF background document on Cybersecurity Culture, Norms and Values Klée Aiken (APNIC), Deborah Brown (Association for Progressive Communications), Anriette Esterhuysen (Association for Progressive Communications), Ryan Johnson (Access Partnership), Dr. Joanna Kulesza (University of Lodz, Poland), Dr. Andrii Paziuk (Taras Shevchenko National University), Dr. Alejandro Pisanty (National Autonomous University of Mexico), Ben Wallis (Microsoft); the numerous contributors and active participants to the BPF discussions on the mailing list, during virtual meetings and at the BPF session during the IGF Meeting in Paris for their involvement, input and feedback; the panellists on the IGF Workshop; all who contributed to the content of this document by submitting formal contributions (as listed in part II).

PART I: Cybersecurity Culture, Norms and Values

Culture, norms and values

On January 31st, 2003, the UN General Assembly adopted Resolution 57/239, noting that all operators and owners of internet technologies should be aware of relevant cybersecurity risks, with respect to their roles. The resolution was titled "Creation of a global culture of cybersecurity", and called upon Member States and relevant international organizations should develop within their societies a culture of cybersecurity.

This message has been echoed and repeated by several organizations. The report of the 2015 IGF Main Session on Cybersecurity called for:

"A culture of cybersecurity is needed on different levels. Individual action was encouraged to make the Internet safer. Moreover, a need for a comprehensive approach to tackling cybercrime and building trust, such as the introduction of security elements when developing cyber products and services, was highlighted. Participants also stressed the critical role that education plays in addressing cybercrime issues and noted that education should be expanded to involve all levels of society. Capacity building was cited as an indispensable driver for cybersecurity".

Sociologists Schwartz and Davis (1981) helpfully define organizational culture as "a pattern of beliefs and expectations shared by the organization's members. These beliefs and expectations produce norms that powerfully shape the behavior of individuals and groups".

Cybersecurity culture in particular has been the subject of recent investigation, including by the European Network and Information Security Agency (ENISA) in February of 2018. ENISA's findings recommended getting buy-in at executive levels, knowing the organization, measuring current levels of security, and building on existing levels of dissatisfaction to drive improvement. Most of this research has been focused on how to apply a culture of security within one organization. Studies at an international level that incorporate wider cultural differences are more rare.

One area of recent development where these distinctions can be observed is in the development of international cyber norms. This paper will focus on the development of norms, places where they can emerge, and draw from some examples to illustrate currently understood best practices. The reader is invited to build on these best practices, and join the Best Practices Forum mailing list to share them ahead of a final document, which will be published after the IGF meeting in Paris, November of 2018.

Background on norms development

Katzenstein (1996) defined norms in a now widely accepted definition as "collective expectation for the proper behavior of actors with a given identity." The development of norms requires a shared belief about proper behavior for actors (in political science, usually states) in a community.

International legal norms guide behavior by creating a framework for mutual expectations and regulating states' behavior. They do not have explicit legal implications, but can often guide the development of international law. Norms are not always adopted with the level of formality that is usually associated with a documented consensus, but may be codified in international law or policy once they see widespread acceptance and support. Social norms of behaviour exist, and can apply to other groups than states. They are not legally binding but regulates behaviour by motivation.They may also be adopted in consensus by a smaller community, but adhered to or supported by a wider community.

The development of norms is marked by three phases: the emergence of norms, the cascading adoption of norms, and the internalization of those norms.

In the emergence phase, we see the realization that a norm is necessary, and the offering of a variety of norms from a variety of actors. We call these early-stage authors of norms "entrepreneurs" because they are responding to an emerging need, without necessarily having a status as an authoritative body for issuing norms on the topic in question. This tends to create a lot of norms early on, many of which don't survive to widespread adoption. It's a bit of trial-and-error to determine where consensus can be achieved.

Once a variety of these proposed draft norms are published and their stakeholders or affected parties have a chance to think through their relative merits, a few of the widely agreed upon norms are adopted in informal and formal ways by the international community. We call this phase the cascade. In the final phase, norms are understood, and enforcement mechanisms may be put in place to help keep states in line with the norms. While codification of norms through these mechanisms typically occurs, these more formal methods of recognition are not needed for a norm to see more widespread adoption or implementation.

In cybersecurity specifically, there has recently been an increase in the number of norms stated and discussed. These new emerging norms come from different sources, and have varying levels of backing from their communities, which may create collisions as well as gaps. In addition, some norms may have been developed in small groups, or closed doors meetings, which is not conducive to increasing their legitimacy.

This emerging trend has produced norms, or at least drafts thereof, in the multilateral arena:

- The UNGGE (United Nations Group of Governmental Experts) represents the highest level in this class, as the GGE originates in the UN General Assembly.

- Other multilateral sets of norms are emerging in regional organizations or mechanisms (like the Shanghai Cooperation) or "club" types of organizations (like the Organization for Economic Co-operation and Development, OECD.)
- The International Telecommunication Union (ITU) is also sometimes seen as contributing to norm formation in cybersecurity, through Resolutions such as PP-45 and other instruments. Although there is contention as to the appropriate role, if any, the ITU has in cybersecurity matters, by developing concepts such as the Global Cybersecurity Index as well as prescriptive models for the drafting of national cybersecurity strategies and incident response team development, the ITU is contributing to the normative dialogue in this space. For example, in conducting capacity building efforts using these set models the ITU is one of many voices that is contributing to a process to define what it means to be 'cyber mature' and guiding the development of policy and institutions based on these guidelines.
- In addition, norm entrepreneurs from other organizations like the Global Commission for Stability in Cyberspace as well as private sector actors are developing norms which they provide for the international community to adopt.

Certain approaches to norms in Cybersecurity, or Cyber Norms, tend to focus on states as main actors; states would be the attackers or defendants, and the entities signing cooperative instruments that enshrine the norms. Some of these norms are implemented or supported in the context of Confidence-Building Measures (CBM). However, the realm of norms development is not uniquely a state activity. Companies such as Microsoft have also proposed cybersecurity norms, including those which apply to private sector organizations. Some organizations, such as the GCSC, have proposed norms that address both state and non-state actors. In this document, we will assume that norms can be proposed, identified and implemented by a variety or communities, including states, international organizations, private sector and civil society.

As large portions of internet infrastructure are operated by private sector organizations, and internet content may be developed and owned by a variety of stakeholders, including citizens, the scope of norms can also imply authorizing, controlling or preventing actions of those other stakeholder groups. When states agree to cooperate on cybercrime, with limited exceptions (state-sponsored cybercrime) they are cooperating on actions taken by individuals and other legal entities, which are not states.

At the national level, Cybersecurity norms also exist. They generally encompass law (general and specific), terms of use, cooperation agreements among sectors such as armies, navies, banks, law enforcement, ISPs and organizations of business and civil society. Some of these norms are being made more uniform across boundaries due to international cooperation or the normative impact across the world of region-specific legislation.

Norms can also arise, often at a less formal level, within industries or communities. As one example, in 2011, the National Institute of Standards and Technology (NIST) in the United States published the "Cybersecurity Framework", as a voluntary framework of guidance,

standards and best practices to manage cybersecurity risk. During the release of an updated version in 2018, US Secretary of Commerce Wilbur Ross flagged that "(adoption of the framework) is a must do for all CEOs" (NIST, 2018). Quotes such as these indicate the normative value of the framework. Participation in organizations such as Information Sharing and Analysis Centers (ISACs) can, due to the size of their community, be considered a norm for a specific sector. This is especially noticeable in Financial Services, where the FS-ISAC was implemented in response to the 1998's Presidential Directive 63 on Critical Infrastructure protection. Today, FS-ISAC has nearly 7,000 members globally sharing cyber threat information (FS-ISAC, 2018).

The case for cyber norms

In terms of effectiveness, an important question to ask is why norms develop. In particular, as there are a number of organizations identifying and proposing norms, giving clear thought to the incentives organizations have for doing so is relevant and important. Especially when norms development happens in closed meetings, such as is the case with the UNGGE's efforts, these can often be less clear.

At a high level, norms are driven by a goal to increase predictability, trust and stability -- with as a main goal to steer away from conflict due to misunderstandings (Osula and Röigas, 2016).

At a more tactical level, development of a specific norm is often driven by more immediate needs. These are not always clearly documented by the organization proposing the norm.

In the case of internet governance, there is a case for norms specifically because the internet is not developed, maintained or governed or managed by any one stakeholder group nor is it contained by national boundaries. This creates a jurisdictional and policy-authority lack of clarity, which can best be filled by norms. There is a parallel between the development of "internet governance" as a concept, and how lack of clarify in internet governance was responded to by the development of different sets of "internet governance principles" and the development cybersecurity as a concept, and the emergence of cybersecurity norms.

For instance, when the UNGGE proposed a norm in 2015, that states should not attack the Incident Response Teams of other states, they did not include a clear reasoning. However, internally to their consensus document, they also encouraged all states to develop their incident response capability to identify and respond to attacks within the state. If those capabilities are not protected, an international incident or disagreement that results in a cyber attack, may make it impossible for the state to respond to critical security incidents on their domestic infrastructure. This may have both implications for the state itself, as well as impair its ability to prevent its infrastructure from being used in attacks on third countries.

The idea that the internet as a whole is very connected, and relatively small attacks in certain parts of the network may impact a much greater set of users, is intrinsic to the concept behind norms development. As an example of this, Microsoft proposed a norm for states to not backdoor software or software update mechanisms. Even though a state may do so in a very targeted way, the concept that software updates are a powerful venue of attack could lead to organizations distrusting these mechanisms, and significantly increase the overall vulnerability of the internet - as organizations may decide to no longer automatically update and no longer get security patches.

Norms development processes

In international relations dealing with cybersecurity the traditional intergovernmental regime is accompanied by specific multi-stakeholder governance. While not unique to cyberspace, the principle of multistakeholderism is one of the pillars of Internet governance, as defined by the Tunis Agenda (WSIS, 2005). It relies on bottom-up processes, resulting in low-level mechanisms and norms, a large number of which are within the field of Internet governance.

To be more specific: Internet governance relies on multistakeholderism – a distributed policy making model based on voluntary cooperation of key actors, usually identified as: states, the private sector[4] and civil society, operating "in their respective roles" through "rough consensus and running code"[5]. While the balance of the multistakeholder agreement depends greatly on the networks in question (in some countries, major parts of the network may be operated by the government, in others by private sector), a single stakeholder group rarely controls a large portion of the global network.

In addition to being mostly bottom-up, and multistakeholder, governance of the internet is also typically seen as "distributed". Distributedness refers to how spaces of internet governance are distributed across sectors and geographic boundaries, including regional, national and global spaces, as well as intergovernmental spaces and those of non-state actors, such as industry, the tech community or civil society. It's not just about who participates, but the spaces where they have the ability to participate. Verhulst et al. make a case that this can enable Flexible and innovative decision-making mechanisms, and ultimately can promote participation (Verhulst, 2014).

This bottom-up, multistakeholder and distributed approach, although neither new or unique to cyberspace, significantly differs from traditional national law making or international norm development. While in both of those scenarios it is states who play a key role, Internet

[4] The Tunis Agenda refers to the private sector rather than business when defining the roles of different stakeholder groups. Private sector is a broader term, and can also include 'technical' private sector actors.

[5] The phrase is a shorthand allusion to the decision making processes within the bottom-up models of governance, specific to the original technical communities behind the global network, with time adopted as the fundamental guideline for all Internet governance related decision making models. See Clark (1992).

governance typically grants national governments and institutions a complementary role in setting and enforcing "principles, norms, rules, decision making procedures and programs" for the global network (Drake, 2009). Recent developments, such as increased internet filtering, internet shutdowns, and censorship have however impacted this balance. The impact of these depends significantly on the individual nation state.

Although a similar, supporting rather than leading, role of states can be witnessed in many other areas of international law and relations, like environmental protection, production of pharmaceuticals or banking, where much is left to good business practice, civil society input and/or consumer choice, the interplay of governments, companies and individuals is nowhere more complex, abundant and transnational than online.

This is likely due to four factors:

- the complexity and scale of online interactions, with 3,6 billion Internet users worldwide in 2017 (ITU, 2017);
- the historical decisions by many governments to allow the Internet to be first and foremost a commercial space[6] which has created a clear precedent of multistakeholder collaboration in the development and governance of the Internet and the underlying systems that support it;
- the gross value of the online market, estimated at 2.304 trillion USD in online transactions globally in 2017 (eMarketer, 2017); and
- the growing extent to which non-internet specific policy and regulatory processes are having to address internet-specific matters. From education to trade, to human rights, to intellectual property, the scope and amount of actors involved continuously increases.

The lines between roles of individual stakeholders are nowhere more controversial and disputed than in the online environment. The norm setting power is shifting away from states, who are trying to regain it at a time of political and economic insecurity. In their attempts to do so they need to consider the networks' specifics: its architecture, design and, most significantly, the particular traits of its current multistakeholder model of governance.

The Internet Corporation for Assigned Names and Numbers (ICANN) is an example of an organization that aims to embody and implement the principle of multistakeholder policy-making. As per ICANN Bylaws (sec. 1.1) its mission is to "ensure the stable and secure operation of the Internet's unique identifier systems". ICANN offers "registration services and open access for global number registries", working closely with the Internet Engineering Task Force (IETF) and Regional Internet Registries (RIRs). Its Bylaws explicitly state that ICANN is not to "regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide", holding no "governmentally authorized regulatory authority". Despite holding no rule-making power

[6] Such as the 1998 decision of the Clinton administration in the US to transfer control of DNS from DARPA and NSF to the Department of Commerce.

ICANN and the community around it sets norms for the global cybersecurity community, not only through contractual compliance but also through standard setting and community consensus. As a result, ICANN is a key participant in the overall governance model of the internet.

A multi-stakeholder governance, bottom-up[7] decision-making process is also present in other technical settings.

They range from technical standards from the IETF and IEEE (including RFCs for BCP or Best Current Practice) to the actual operation of CERTs and CSIRTs. For instance, within the CSIRT community, and in particular the Forum of Incident Response and Security Teams, standards have been published on the types of services CSIRT typically operate. In addition, an Ethics working group has been established among CSIRTs to identify appropriate behaviors for CSIRTs.

Participants in norm-setting and in implementation and operation are not only state actors, but all stakeholders, from technology developers through network and system sellers and operators to businesses, civil-society organizations, and ordinary citizens. The organized forms of this regime are organizations such as the Mail, Messaging, and Malware Anti-Abuse Working Group (M3AAWG) and Anti-Phishing Working Group (APWG).

The everyday regime of constant attacks, risk management, attack response and recovery often works well within the multistakeholder regime even before a full set of norms is put into place. Many of the norms we now know have been established after experience. The organizations listed above often do not always see themselves as defining norms, but play a crucial role in developing shared understandings and agreement on what is responsible behavior, and what is not.

One clear area where a shared understanding is developed is through international law. Examples include the EU's Directive on Security of Network and Information Systems (NIS Directive), or the EU's General Data Protection Regulation (GDPR), in which EU member states develop a shared understanding and requirements. Due to the market size of the EU, these laws often have repercussions beyond the place where they are directly applicable. As such they lead to discussion on behaviors, and inform the more formal norms development processes discussed in the remainder of this document. In many ways, international "hard" law can often be seen as the original norms development arena.

[7] It should be noted that while a multi-stakeholder model can be designed to be "bottom-up", but not always is. "Bottom up" does not necessarily mean that a diversity of stakeholders is involved.

Spaces for norms development

Who can create cyber norms?

Nearly all states and international organisations can be norms creating bodies, especially if they deal with international trade or transnational activities such as banking. Their "norms" are directly applicable to the online environment, just to mention the EU NIS Directive or GDPR. In that respect, all international organisations can be norms developing organisations, relevant to cybersecurity. Other organizations have also specifically identified themselves as being norms developers or promoters. These include initiatives such as the Global Committee on the Stability of Cyberspace, the UNGGE, companies like Microsoft, and others.

Specific examples of norms creators

- **UN Government Group of Experts (UNGGE):** the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security is a UN mandated group of experts which has been established five times since 2004. It is convened under the UN's First Committee. The GGE will meet for four one-week sessions. When consensus is reached, the group publishes an outcome report, which has happened in 2010, 2013 and 2015. In particular the 2013 and 2015 edition discussed norms development, with the 2015 report offering a proposal for voluntary cybersecurity norms. Outcomes and inputs to the UNGGE process have been echoed by other bodies, showing some level of adoption. For instance, the US Coordinator for Cyber Issues, Christopher Painter, referred to several UNGGE norms in a testimony before the United States Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity (Painter, 2015). They were also referred to in the Leaders Communique of the G20 Antalya summit (G20, 2015), by ASEAN Ministers and member states since 2017, and in numerous national cyber-related strategies, including the Australian International Cyber Engagement Strategy (2017).

  In its last iteration, the 2016-2017 UNGGE did not achieve consensus, and did not publish a report.

- **Global Commission on the Stability of Cyberspace (GCSC):** initiated by two independent think tanks, The Hague Centre for Strategic Studies (HCSS) and the EastWest Institute (EWI), the GCSC consists of 26 prominent Commissioners from a variety of regions and stakeholder groups, and legitimacy in different aspects of cyberspace. Its aim is to help promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity. As a group, it has proposed a number of norms for responsible behavior in cyberspace.

- **NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE):** In 2016, the CCDCOE, based out of Estonia, convened a group of legal experts and facilitated a second version of the Tallinn Manual, an assessment of how international laws, treaties and norms regulate activities in cyberspace. The original version of the document, published in April of 2013, was the first major effort to interpret international law in the context of cyber operations, and by offering guidance on reasonable interpretations of the law, developed normative content.

- **Microsoft:** since 2013, Microsoft has taken a strong industry role in support of international cybersecurity norms development. These contributions have ranged from outlining five principles for developing norms, through six proposed norms in 2016 and most recently the proposal for a Digital Geneva Convention to protect Cyberspace (Microsoft, 2017).

- **Bilateral Agreements:** Voluntary or binding bilateral agreements have been identified as a means to develop, demonstrate, and socialize norms. For example, the 2015 U.S. China Cyber Agreement set forth, among other things, that the two countries would refrain from cyber-enabled theft of intellectual property. The agreement itself represented a strong normative statement, defining what is and is not acceptable behavior for a responsible actor on the international stage and the noted decline in this type of IP theft suggested an even wider impact. The echoing of the agreement's language in subsequent bilateral agreements including between the US and South Korea, the UK and China, Australia and China, and even in the 2015 G20 Leaders Communique all exemplify norm proliferation.

- **Unilateral Action:** Unilateral action can be a means for states and other actors to define what they view as appropriate and inappropriate behavior, acting as norm entrepreneurs. The most common means of doing this can be in public statements and the publication of doctrines or strategy that clearly articulate an actor's position on cyber matters. A recent trend in the public disclosure of when and how some states will use their offensive capabilities is an example of this, where the guidelines serve to outline that states view on what a responsible use of offensive cyber capabilities is, set positions, define intentions, and push the conversation forward.

  More forceful action such as indictments and sanctions can also be unilateral tools to develop norms. The US indictments of five PLA officers in 2014 and the sanctions on North Korea that followed the Sony Hack fall in this category, where the expectation of arrests or meaningful economic costs were low, but the tools were used to set precedent and indicate the US perspective on the acceptability of certain activities. The link between the 2014 indictments and the eventual 2015 US-China Cyber Agreement could be suggestive of the potential normative impact of unilateral action.

- Centered on human rights, a coalition of 30 governments partnered on the **Freedom Online Coalition**, which published a set of recommendations for human rights based approaches to cybersecurity (FOC, 2011). In addition, the United Nations Human Rights Council published resolutions that touch on State approaches to security and internet policy (see PP12, PP14, OP8 and OP9 of HRC/RES/38/L.10/Rev.1 for example) In addition, UN Special Procedures have issued reports that are discussed by States at the HRC and UNGA, and which contribute to norm developments relevant for cybersecurity.

- **Groups and associations often aim to identify norms**, either applicable to their own community, or to others. Organizations frequently have Ethics charters that apply to their membership, which may be enforced or voluntary. Experts or interested parties may also identify proposed norms and seek to see them universally accepted. An example of this is Necessary and Proportionate, a set of "International Principles on the Application of Human Rights to Communications Surveillance", which aim to apply existing human rights law to digital surveillance. These were originally developed by a coalition of experts in civil society, and were subsequently endorsed by organizations and individuals.

- At a regional level, the **African Union** published its Declaration on Internet Governance, with provisions on cooperation in cyber security. However, these provisions were very light and defer to other agreements such as the Malabo Convention co combat cybercrime, and the African Union Convention on Cybersecurity and Personal Data Protection (KictaNet, 2018). Another relevant regional initiative is the **Shanghai Cooperation Organization (SCO).** The SCO is an intergovernmental organisation created in 2001 by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. India and Pakistan joined SCO as full members on June 9th, 2017. In 2009 they published an "agreement on cooperation in the field of ensuring the international information security". In 2011, the organization submitted to the UN General Assembly a proposal for an International Code of Conduct for Information Security. In 2015, the proposed code was updated and now includes reference specifically to a need to understand how the norms development work happening in the UNGGE will apply to state behavior.

Due to the nature of norms development, not all new norms need to be pronounced as such, as is the case with the above organizations.

Norms develop and appear when their stakeholders roughly agree, and can sometimes be observed through the reaction of other states to state behavior. As a result, the above list is not exclusive, and norms development will grow over time through the efforts of many participants, and often driven by external events.

Potential for emerging norms developers

A new group of norms may emerge from the financial sector and related organizations like the IMF and WEF. This can be expected in response to the recent (2017-18) spate of attacks to banks, Central Banks, and payment systems such as occurred against Bangladesh, Mexico, and Chile.

As one specific example, the Carnegie Endowment for International Peace recently urged States, and in particular the G20, to pledge refraining from "(activities which) undermine the integrity of data and algorithms of financial institutions in peacetime and wartime" (Schmitt, Maurer, 2017).

In the case of Mexico, news by end of June 2018 suggest that the payment system was compromised with the aid of insiders. The fact that this part of the attack happened in-country may have been instrumental in accelerating the country's adhesion to Convention 108, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", and put into action closer collaboration in the banking sector.

Norms are at present developed variously by government, intergovernmental organizations, private sector, civil society groups, the technical community and industry coalitions. A notable absence, with some exceptions, such as norms initiatives that permit individuals to subscribe through a signature or other method of public support, are users and user groups, who are ultimately affected by the norms that are developed.

State of existing norms development and implementation

Examples of proposed norms

The following are examples of proposed norms, or normative language which have been developed by a number of organizations and associations. This lis is not exhaustive, and the degree to which a statement can be perceived as a norm, due to the lack of concrete and formal unanimity, is sometimes debatable:

- **UNGGE:** In 2015, the UNGGE released a report including international legal principles humanity, necessity, proportionality and distinction (Paragraph 28c), which is corresponding to the principles of the international law of armed conflicts. It also like 2013 Report reaffirms application of the UN Charter with it's basic principles of state behavior "online like offline". In the document, it proposed a list of 11 voluntary, non-binding norms. Some of these restricted state behavior, whereas others compelled states to help during an incident. An example of either include (UNGA, 2015):

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

"States should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity"

- **GCSC:** In November of 2017, the GCSC proposed its "call to protect the Public Core of the Internet". This call urged actors to avoid actions that would "intentionally and substantially damage the general availability and integrity of the public core of the Internet". While there was no concrete definition included of this "public core", associated research was released which drove discussion, and included examples such as attacks on the Domain Name System, forging of digital certificates and corrupting certificate authorities (GCSC, 2017). In May of 2018, the GCSC proposed an additional norm to protect election infrastructure from cyber operations: ""*State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites*". (GCSC, 2018).

- **Tallinn Manual:** The Tallinn Manual 2.0 indicates that there are overarching international law principles relevant to cybersecurity policy and international practice: 1) sovereignty, 2) jurisdiction, 3) state responsibility, and 4) due diligence.

  While the notion of 1) sovereignty and 2) the matrix of jurisdictional principles remains an unresolved challenge for Internet governance and critical infrastructures protection, subject to enhanced debate and still far from consensus, the two other principles of international law: 3) state responsibility and 4) due diligence can be easily applied to the biggest international open network and its key components.

- **Microsoft:** Microsoft proposed a set of norms in three categories (Microsoft 2015, 2015a)
  - Those that govern offensive behavior, and reduce conflict. An example of a propose norm in this area is "*States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and service.*"
  - Those that govern defensive behaviors, and manage cybersecurity risk. An example includes "*States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace*".
  - Those that govern industry, and in particular global ICT companies. They state: "*Companies must be clear that they will neither permit backdoors in products nor withhold patches, either of which would leave technology users*

exposed".

- The **Organization for Security and Co-operation in Europe published** OSCE DECISION No. 1202 on CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES. This document included several Confidence Building Measures, such as the commitment to voluntarily share information on measures they have implemented to ensure an open, interoperable, secure and reliable internet, and the nomination of a contact point for communications and dialogue on security in the use of ICTs (OSCE, 2016).

- The **Association of Southeast Asian Nations (ASEAN)** in 2015 published a Regional Forum Work Plan on Security and the Use of Information and Communication Technologies (ICTs). While being short of a solid commitment by individual ASEAN states, this document proposed a number of activities that align with wider norms, such as the voluntary sharing of information, promotion of research, and wider discussion of rules, norms and principles (ASEAN, 2015).

- The **Shanghai Cooperation Organization (SCO)** published its "Agreement between the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security" in December of 2008. It specified main areas of cooperation, including countering threats of using ICTs for terrorism, countering information crime, exchanging expertise and training. (CCDCOE, 2018).

- The **BRICS** countries, at their Fortaleza summit, issued a Declaration in 2017, which noted its intent to explore cooperation on cybercrime, and the establishment of a group of national security advisors to explore practical proposals for cooperation and coordination of their activities in international fora (University of Toronto, 2014).

- **As mentioned, the G20** included Cyber stability measures in its "G20 Leaders' Communiqué, Antalya Summit,". For instance, the declaration stated "no country should conduct or support ICT-enabled theft of intellectual property" (G20, 2015).

- In Civil Society, examples of norms approaches include an initiative by the Association for Progressive Communications (APC) and other civil society organizations at the 2017 to launch a "**rights based approach to cybersecurity**" (DigitalWatch, 2017). The core concern of this effort is that human rights and cybersecurity should be seen as interdependent and complementary rather than conflictual. Another example is the **Manila Principles on Intermediary Liability**, developed by several Civil Society groups including the Electronic Frontier Foundation and Article19 (Manila Principles, 2015).

- The Internet Society has driven many Technical Community participants to support the **Mutually Agreed Norms for Routing Security** (MANRS, 2016).

Norms implementation

Norms are only successful at driving responsible behavior in cyberspace when they are successfully implemented. Implementation of a norm needs to consists of driving awareness, building acceptance and monitoring to what degree it is accepted.

An easily identified example that hampers the success of norms as a tool of driving responsible behavior is that of attribution. While a norm may prescribe a specific cyber attack to not be acceptable, if it is not possible to identify who violated the norm, anyone can subscribe to the norm while still actively violating it. This gives such a state the benefits of international acceptance, without the costs of other states being able to respond to the violation of the norm.

As a result, implementation measures are critical to the success of norms. However, while norms development is widely described, few best practices are available regarding the implementation of norms. This chapter calls out a few examples of implementation efforts.

- Singapore's leadership in ASEAN this year focuses on Norms. In October of 2017, a statement on behalf of ASEAN by Joseph Teo, Deputy Permanent Representative of Singapore to the United Nations called out specifically ongoing work within ASEAN to forge consensus on global norms on cyberspace. Singapore has specifically invested in Confidence Building Measures, including Singapore International Cyber Week to facilitate dialogue around cybersecurity issues.
- Alex Grigsby (Grigsby, 2017) has published, in the GCSC's Issue Brief number 1, a mapping of existing cyber diplomatic efforts, including an overview to what degree states refer to norms development as necessary to promote stability and their key stated concerns. This level of clarity helps participants in the global norms debate understand to what degree norms and their underlying conversations are gaining traction (GCSC, 2017).
- The Carnegie Endowment for International Peace has developed a Cyber Norms Index, which maps language used to identify international law as well as aspirational norms under development in the community. It also maps language specific to Confidence Building Measures and Capacity Building to support these norms.
- Microsoft has proposed the development of an independent and international attribution agency that could examine specific attacks and share evidence showing where a given attack was by a specific nation-state. Such an agency could strengthen the community's ability to apply norms and respond effectively to violations of these responsible behaviors.

Digital security divide

In a 2016 publication, the Internet Society launched the concept of digital "security and trust divide". In their words: "cyber threats will continue to multiply and users who lack the skills, knowledge and resources to protect themselves and their data will be far more likely to become
victims of cybercrime". Whether the individual has access to these skills, knowledge and resources is often associated with financial and/or education gaps. Gaps can also exist between countries, along many different dimensions: capacity; resources; vulnerabilities; and also divides emerging from whether they choose to invest in offense or defense.

Stakeholder groups often have the ability to mitigate or increase these gaps through coordinated action. For example, if a state implements data protection laws and has competent data protection authorities in place, people will be exposed to less risk irrespective of their own skills and knowledge. Governments can also contribute to digital insecurity of individuals by requiring them to provide their biometric data in order to gain access to critical public service, and not managing this data in a secure manner. For instance, in India, there have been multiple reports during the year of data breaches involving the biometrics-based identification system Aadhaar. In May 2017, it was reported that the Aadhaar numbers and personal information of as many as 135 million Indians could have been leaked from four government portals due to lack of IT security practices. There were additional reports during the year of government websites inadvertently publishing personally identifiable information, including names, addresses, bank information and Aadhaar numbers, thereby making them available to the general public (Privacy International, 2017). It's not only the government that can step in: Individuals are often blamed for not installing updates, however a recent study on Android vulnerabilities found that it is device manufacturers that fail to provide updates to users in order to fix critical vulnerabilities, rather than users failing to install them (Thomas, Beresford, Rice, 2015).

However, one interesting question that arises with norms is to what degree norms provide security value to citizens and constituents of organizations that subscribe to a specific norm.

As an example, citizens of a country that subscribes to and supports the UNGGE norm "States should take appropriate measures to protect their critical infrastructure from ICT threats" will benefit from norm implementation measures the state takes, such as the development of an incident response capability for the critical infrastructure sector.

It's also important to recognise that digital insecurity is not experienced evenly amongst citizens of a country. People who face discrimination on the basis of gender, race, religion, sexual orientation or gender identity, age or other factors can face much more severe consequences if they are targeted by a cybercriminal or attack. When their data is not secure, it can be exploited and used to discriminate, harass or incite violence against them. This is another form of a digital security divide.

In addition, users of software published by a vendor subscribing to the proposed Microsoft norm that "ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives" benefit from protection from governments, including their own, that does not subscribe to this norm.

Due to its global nature and multi-stakeholder constituency, the BPF is in a privileged place to call upon its participants for examples of where the unequal application of a norm can reduce security for portions of the wider user base of the internet. In addition, the implementation of said norm, and the availability of rights and protections, accountabilities and remedies can also impact users significantly. Examples of these challenges can lead to a better understanding of how norms can concretely improve security.

An additional, related research question is to what degree some states may actually benefit from not addressing their own cybercrime and cyber security challenges. By having unclean networks, attacks emanating from the country may more easily be considered related to "criminal actors" rather than be indicative of state behavior. In addition, some states may monetarily benefit from specific online criminal activity, and thus not be incentivized to take part in the global norms debate, or implement its outcomes.

Norms also should be considered in terms of the communities they affect. For instance, a norm related to the security of personal data may implement a minimum standard across a wider population group, without taking into account the specific threats faced by minority groups or groups who face forms of discrimination. As a result, that group may be less protected by the same norm, than a population majority. This may exacerbate an existing digital security device.

As an example, women and people who face discrimination on the basis of sexual orientation and gender identity may be disproportionately affected by inappropriate design or implementation of a norm protecting individual information.

There are two reasons for this:

- The first relates to the consequences of data breaches of sensitive personal data can be much more severe for at-risk or marginalized communities. For example, in Sao Paolo, Brazil, a database containing the records of 650,000 patients was made public, putting people at a variety of risks, from becoming victims of identity theft to persecution e.g. when the identities of women undergoing abortions were exposed. Abortion is almost always a crime in Brazil, punishable by up to three years in jail, and there is no exception for defects caused by the Zika virus. Consider also the consequences for an individual whose sexual orientation is exposed when they live and work in countries where being gay, lesbian or bisexual is illegal?
- The second reason is that women and people who face discrimination on the basis of sexual orientation and gender identity are already vulnerable online because they are often proactively targeted by malevolent actors. They already face cyberstalking, and

threats of rape, or death threats - which often extend to their families - and threats of non-consensual dissemination of intimate or sexual content. Their email accounts, mobile phones, or other electronic devices are frequently hacked and they are subject to doxxing. Technology-related violence against women cause psychological and emotional harm, reinforce prejudice, damage reputation, cause economic loss and pose barriers to participation in public life, and may lead to sexual and other forms of physical violence.

Norms that intend to promote individual security, and that require actions of states and other actors such as service providers to do so, need to take the specific circumstances of groups at risk into account.

Bibliography

Alexander Klimburg, The Darkening Web - The War for Cyberspace, Penguin Random House, 2017

Anna-Maria Osula and Henry Röigas (Eds.) International Cyber Norms - Legal, Policy & Industry Perspectives, CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) Tallinn, Estonia, 2016

Ben Buchanan, The Cybersecurity Dilemma - Hacking, Trust and Fear Between Nations, Oxford University Press, Oxford

Carnegie Endowment for International Peace, Cyber Norms Index. Retrieved, July 3rd from https://carnegieendowment.org/publications/interactive/cybernorms

J. Kulesza. Due diligence in international law, BRILL 2016

J. Kulesza, R. Balleste (eds). Cybersecurity and Human Rights in the Age of Cyberveillance, Rowman & Littlefield 2016

J. Kulesza. International Internet Law, Routledge 2012

J. Kulesza, R. Weber. Protecting the public core of the Internet [in:] Contribution from the Research Advisory Group, GCSC Issue Brief 1: Briefings and Memos from the Research Advisory Group, The Hague Centre for Strategic Studies 2017, 75

J. Kulesza. Cybersecurity due diligence: lessons learned from international liability law [w:] Advanced Cyberlaw and Electronic Security (red. I. Vasiu, F. Streteanu), Accent 2017, 62-80

J. Kulesza. Pre-emptive cyberattacks in international law [in:] NATO Road to cybersecurity, J. Świątkowska (ed.), Kosciuszko Institute 2016, 17-27

J. Kulesza. Due Diligence in Cyberspace [in:] Organizational, Legal, and Technological Dimensions of Information System Administration, I. M. Portela, F. Almeida (eds.), IGI Global 2014, 76

J. Kulesza, R. Balleste. Signs and Portents in Cyberspace: The Rise of Jus Internet as a New Order in International Law, Fordham Intellectual Property, Media & Entertainment Law Journal 2013, 1311

J. Kulesza. Towards and Internet Framework Convention: The State of Play, Hague Yearbook of International Law, 2013, 84

Klée Aiken. Ready to Respond to the Cyber Norms Debate, FIRST Blog, 2018. Retrieved, July 6 2018 from https://www.first.org/blog/20180423-cyber-norms.

Microsoft, From Articulation to Implementation: Enabling progress on Cyber Norms. Retrieved, July 4th from https://www.microsoft.com/en-us/cybersecurity/content-hub/enabling-progress-on-cybersecurity-norms

Pablo Hinojosa et al. Workshop on Cybernorms and Internet governance, IGF Guadalajara 2016

Ryan Johnson. Norms for Cybersecurity in Southeast Asia, Access Partnership, 2017. Retrieved, July 4th 2018 from https://www.accesspartnership.com/norms-cybersecurity-southeast-asia/.

UNIDIR. The United Nations, Cyberspace and International Peace and Security: Responding to complexity in the 21st century. Retrieved, July 4th from http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

UNODA. Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary. Retrieved, July 4th from http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Van Horenbeeck, Maarten. An Internet of Governments, USENIX LISA '17. Retrieved, July 4th 2018 from https://www.usenix.org/conference/lisa17/conference-program

Van Horenbeeck, Maarten. Norms development in regional political associations. Retrieved, July 4th from https://www.daemon.be/maarten/cybernorms.html

References

ASEAN (2015). 2015 ASEAN REGIONAL FORUM WORK PLAN ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES. Retrieved, July 15th 2018 from https://cil.nus.edu.sg/wp-content/uploads/formidable/14/2015-ARF-WP-on-ICT-Security.pdf.

Schmitt, Maurer (2017). Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?. Retrieved, July 15th 2018 from http://carnegieendowment.org/2017/08/24/protecting-financial-data-in-cyberspace-precedent-for-further-progress-on-cyber-norms-pub-72907.

CCDCOE (2018). Shanghai Cooperation Organization. Retrieved, July 15th 2018 from https://ccdcoe.org/sco.html.

Drake (2009). 'Introduction: The Distributed Architecture of Network Global Governance' in William J Drake and Ernest J Wilson (eds), Governing Global Electronic Networks (Cambridge, Massachusetts: MIT Press, 2009) 8-9.]

DigitalWatch (2017). A Rights-Based Approach to Cybersecurity. Retrieved, July 15th 2018 from https://dig.watch/sessions/rights-based-approach-cybersecurity.

eMarketer (2017). Worldwide Retail and Ecommerce Sales: eMarketer's Updated Forecast and New Mcommerce Estimates for 2016—2021. Retrieved, July 3rd from: https://www.emarketer.com/Report/Worldwide-Retail-Ecommerce-Sales-eMarketers-Updated-Forecast-New-Mcommerce-Estimates-20162021/2002182.

FS-ISAC (2018). Mission Statement. Retrieved, July 15th from https://www.fsisac.com/about/mission.

FOC (2018). A human rights based approach to cybersecurity. Retrieved, July 15th from https://freeandsecure.online/.

G20 (2015). G20 Leaders Communique agreed in Antalya. Retrieved, July 4th from http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

GCSC (2017). Call to Protect the Public Core of the Internet. Retrieved, July 1st from https://cyberstability.org/research/call-to-protect/.

Grigsby (2017a). BRIEFINGS FROM THE RESEARCH ADVISORY GROUP: Overview of Cyber Diplomatic Initiatives. Retrieved, July 15th from https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf.

GCSC (2018). Global Commission Urges Protecting Electoral Infrastructure. Retrieved, July 4th from https://cyberstability.org/research/global-commission-urges-protecting-electoral-infrastructure/.

Huizer, Crocker (1994). "IETF Working Group Guidelines and Procedures", RFC 1603, March 1994.

IETF (1992). Proceedings of the Twenty-Fourth Internet Engineering Task Force, pages 539-543, July 1992, < http://www.ietf.org/proceedings/24.pdf>

Internet Society (2016). Paths to our Digital Future. Retrieved, July 3rd 2018 from https://future.internetsociety.org/

ITU (2017). Internet usage statistics. Retrieved, July 3rd 2018 from: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

KictaNet (2018). African Union Declaration on Internet Governance. Retrieved, July 15th from https://www.kictanet.or.ke/wp-content/uploads/2018/02/Declaration-on-Internet-Governance_adopted-AU-Summit-2018.pdf.

Osula and Röigas (2016). International Cyber Norms - Legal, Policy & Industry Perspectives, CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) Tallinn, Estonia, 2016

OSCE (2016). Decision No. 1202. OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES. Retrieved, July 15th 2018 from https://www.osce.org/pc/227281?download=true.

Manila Principles (2017). Manila Principles on Intermediary Liability. Retrieved, July 15th, 2018 from https://www.manilaprinciples.org/individual-signatories.

MANRS (2016). Mutually Agreed Norms for Routing Security. Retrieved, July 15th 2018 from https://www.manrs.org/.

Microsoft (2015). Six Proposed Norms to Reduce Conflict in Cyberspace. Retrieved, July 1st 2018 from https://cloudblogs.microsoft.com/microsoftsecure/2015/01/20/six-proposed-norms/.

Microsoft (2015a). The case for International Cybersecurity Norms. Retrieved, July 1st 2018 from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REY05a.

Microsoft (2017). The Need for a Digital Geneva Convention. Retrieved, July 17th 2018 from https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention

NIST (2018). NIST Releases Version 1.1 of its Cybersecurity Framework. Retrieved, July 15th 2018 from https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

Painter (2015). Testimony Before Policy Hearing Titled: "Cybersecurity: Setting the Rules for Responsible Global Behavior". Retrieved, July 4th 2018 from https://2009-2017.state.gov/s/cyberissues/releasesandremarks/243801.htm.

Privacy International (2017). Cyber Security in the Global South. Retrieved, July 15th 2018 from https://www.privacyinternational.org/sites/default/files/2017-09/Cybersecurity_2017.pdf.

Schwartz, H. and Davis, S.M. (1981) Matching Corporate Culture and Business Strategy. Organizational Dynamics, 10, 30-48.

Thomas, Beresford, Rice (2015). Security Metrics for the Android Ecosystem. Retrieved, July 15th, 2018 from https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf.

UNGA (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved, July 1st 2018 from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

University of Toronto (2014). The 6th BRICS Summit: Fortaleza Declaration. Retrieved, July 15th 2018 from http://www.brics.utoronto.ca/docs/140715-leaders.html.

Verhulst, Noveck, Raines and Declerq (2014). Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem. *Global Commision on Internet Governance Working Paper no. 5*. Retrieved, July 15th 2018 from https://ssrn.com/abstract=2563810.

WSIS (2005). Tunis Agenda For The Information Society. Retrieved, July 3rd 2018 from http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

PART II: Report on the public Call for Contributions

Introduction & Methodology

The BPF Background paper, which is included in Part I of this report, was published on the IGF website together with the BPF's *Public call for contributions*.

The BPF Cybersecurity launched a Public call for contributions to gain perspectives from all interested stakeholders on existing norms development efforts, how these norms are being implemented and whether they are successful, and to better understand whether differences in design and implementation may result in a "digital security divide": a group of "haves" and "have-nots" in terms of the protection norms offer.

The Call for contributions was published on the IGF website and contributions were accepted August through mid-October 2018. The BPF received 16 contributions, they are published on the IGF website and summarised in this summary.

Questionnaire

The contributors were invited to provide answers on the following open questions.

1. How do you define a culture of Cybersecurity?

2. What are typical values and norms that are important to your or your constituents?

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms?

4. Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?

5. Do you have examples of norms that have failed (they have not seen widespread adherence), or had have adverse effects (living up to the norm led to other issues)?

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

7. Within your country, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

Contributions

The 2018 BPF Cybersecurity received 16 contributions. All contributions can be found on the IGF website. The numbers [1] … [16] are used as reference throughout this summary report.

[1] The WSIS Coalition (Google, AT&T, Intel, Verisign)
http://www.intgovforum.org/multilingual/filedepot_download/6763/1356
[2] ARTICLE 19 Eastern Africa
https://www.intgovforum.org/multilingual/filedepot_download/6763/1348
[3] Mallory Knodel (ARTICLE 19); Matthew Shears (Global Partners Digital)
http://www.intgovforum.org/multilingual/filedepot_download/6763/1341
[4] The Association for Progressive Communications
http://www.intgovforum.org/multilingual/filedepot_download/6763/1340
[5] Microsoft
http://www.intgovforum.org/multilingual/filedepot_download/6763/1339
[6] CCAOI
http://www.intgovforum.org/multilingual/filedepot_download/6763/1338
[7] Cristina CUOMO
https://www.intgovforum.org/multilingual/filedepot_download/6763/1337
[8] The Cybersecurity Tech Accord
https://www.intgovforum.org/multilingual/filedepot_download/6763/1336
[9] Marilson MAPA
http://www.intgovforum.org/multilingual/filedepot_download/6763/1332
[10] Sudha BHUVANESWARI
http://www.intgovforum.org/multilingual/filedepot_download/6763/1327
[11] Afifa ABBAS
http://www.intgovforum.org/multilingual/filedepot_download/6763/1321
[12] Andrea CHIAPPETTA (Aspisec)
http://www.intgovforum.org/multilingual/filedepot_download/6763/1320
[13] Shreedeep RAYAMAJHI
http://www.intgovforum.org/multilingual/filedepot_download/6763/1310
[14] IEEE Internet Initiative
http://www.intgovforum.org/multilingual/filedepot_download/6763/1350
[15] Anahiby BECERRIL
http://www.intgovforum.org/multilingual/filedepot_download/6763/1324
[16] Global Commission on the Stability of Cyberspace (GCSC)
https://www.intgovforum.org/multilingual/filedepot_download/6763/1372

Summary of contributions

Disclaimer:

the Summary report aims to reflect different stakeholder perspectives that emerged from the contributions submitted to the BPF. Opinions expressed are not those of the editors of the report, nor are they the result of a deliberation and consensus among the participants to the BPF. The report paraphrases and highlights from the contributions elements that are directly linked to the different questions in the Call for contributions. The figures [1] to [16] refer back to the different contributors, their verbatim input to the BPF can be found on the IGF website.

1. How do you define a culture of Cybersecurity?

Contributions reflecting on the general concept

A culture of cybersecurity can be defined as

- An overall **awareness, adequate information and knowledge** of cybersecurity risks and related threats; *[1] [6]*
- A **collaboration among stakeholders**, based on **local values and the perceptions** of different **stakeholders** in the community *[1] [13]*, to identify opportunities and **strategies** to mitigate risks and challenges *[1] [13]*,
  and **techniques to protect** themselves and others from cyber threats by taking precautions following agreed norms and values *[6] [13]*.
- A responsibility to **empower** others in the society **to make responsible cybersecurity choices** by socializing and promoting cybersecurity awareness in the public and private sectors and supporting the development of informed and effective cybersecurity policies. *[5]*

A culture of cybersecurity will enable a **holistic approach** that will enrich the dialogue around cybersecurity and help stakeholders contribute in the most productive ways *[1]*, and necessarily implies an **ethical stance on the part of all actors** to avoid a laissez-faire behaviour without justification *[9]*. As in the 'real world' applicable security rules intend to achieve standards of safety and to reach the highest performance of social order, with the aim to establish **discipline, rationality and coherence among stakeholder interests.** *[7]*

Developing a resilient culture is inherent in a **multi-stakeholder process**, with roles for government, industry, and civil society to support establishment in countries across the development spectrum; to socialise and promote **cybersecurity awareness** in the public and private sectors; and to support the development of informed and effective **cybersecurity policies** in emerging economies. *[8]*

Contributions focusing on human rights and a rights enabling cybersecurity culture

Contributors underlined that **Cybersecurity and human rights are complementary, mutually reinforcing and interdependent** *[3]*. They warn against a cybersecurity debate that increasingly depicts privacy and human rights against public safety and national security, suggesting a trade-off while mutual reinforcement is possible, which is not only misleading, but undermines public safety and security, as well as freedom. *[3] [4]*

Recognising that **individual security is at the core of cybersecurity** means that protection for human rights should be at the centre of cybersecurity policy development *[3];* stakeholders should put **ALL people** (the least empowered as well as the most powerful) **and their rights at the centre** of every **policy decision,** and cybersecurity policies should **respect human rights by design**. *[2] [3] [4]*

A cybersecurity culture that is **human rights-based**, and places the security of users, their data (including users' data shared data in non-digital ways *[2])*, and their online communications at the centre of its concerns is defined by:

- **Trust** in the security of **networks, protocols, devices**; *[4]*
- Respect for **due process and international law** (particularly where human rights law conflicts with corporate interest); *[2] [4]*
- **A systematic approach**, addressing technological, social, and legal aspects together; *[4]*
- **A cross-border approach,** rather than being limited to national security concerns, that does not differentiate between national security interests and the **security of the global Internet**; *[4]*
- Respect for digital **security expertise and training**; no criminalisation of people, their work and the tools used *[4];* processes and policies for the notification of data breaches' and responsible disclosure of vulnerabilities; *[2]*
- Responsibility for all stakeholders and **no disproportionate burden and transfer of responsibilities on individual users**. *[2]*

A cybersecurity culture as an organisation's human firewall against attacks

A culture of cybersecurity in an organisation can be defined as an **intentional internal culture** that prioritizes the cybersecurity of products and customers *[5]* and acts as a **defensive strategy** against threats. *[10]*

The development of a culture of cybersecurity depends on **everyone** *[10]*, starting from the senior management level to each and every staff member, and has **multiple facets** including employee training, audits, "secure by design" process *[5]* etc.

This culture can be inculcated by **making everyone feel that cybersecurity is their own responsibility**, training them to provide an awareness of cybersecurity, and making it an engaging activity and reward with recognition for those who are actively involved in it. *[10]* A culture of cybersecurity is **the attitude, mindset, belief, experience of people regarding cybersecurity**. By adopting this culture, employees of any organization will consider cybersecurity as an integral part of their lives. An organization with good cybersecurity culture tends to have **a strong human firewall** and to be less prone to cyber-attacks. *[11]*

However, in many governments and companies, an effective culture of cybersecurity is still far from being reached due to the lack of knowledge and personnel involved. In several institutions (public and private) the cybersecurity is considered as a branch of the IT department. *[12]*

2. What are typical values and norms that are important to your or your constituents?

General - characteristics, requirements for norms and norms development
One contributor specified the following general characteristics or requirements for cybersecurity norms:

- Be **easy to understand and abide by;**
- Provide clarity of the potential cybersecurity **risks and best practices** to follow;
- Provide proper support through **training** to abide by the norms;
- Create **awareness of the legal provisions** against cyber crime;
- Foresee **regular updates**: (i) at the technical level (patches, updates, etc.) to protect oneself and (ii) information on the latest developments including global best practices. *[6]*

Most of the time, norms are about persuasion, and the persuasiveness of appeals to adopt various norms depends on how they are presented to potential adopters. We learn from experience and adopt during live events and following experiences. Norms can develop in a variety of ways, particularly through habit and the process of adaptation. Some norms emerge spontaneously without any particular actor having any particular intent and then become entrenched through habit. In any group that interacts regularly, norms develop simply through expectations shaped by repeated behavior. *[13]*

A contributor emphasised that cybersecurity values:
1) should provide **security to the company and their customers**,
2) should not be considered as extraordinary costs but as **operational and fundamental** to be in the world markets. *[12]*

Other contributors called for **secure Internet connections**, especially around elections, and no Internet shutdowns. *[2] [3]*

One contributor defines the following values and norms as most important:

- Cybersecurity practices, policies, and strategies must put **human rights at the core**, rather than treating cybersecurity and human rights as inherently at odds with each other.
- **Integrating rights and security:** Promoting a rights-based approach to cybersecurity has to be rooted in both security concerns and human rights concerns.
- **Inclusion:**The norm of transparent and inclusive decision-making is vital and there is no justification for the elitism and exclusion that often characterises decision-making and policy-making related to cybersecurity.
- **Collaborative and multistakeholder approaches:** Governments, civil society and the technical community should work together closely to ensure cybersecurity for all. Civil society and other rights advocates, business and the technical community should recognise the

states' responsibility for protecting the rights and security of their citizens and engage constructively and, when necessary, critically.
- **End-user oriented:** Discussions about cybersecurity should be "humanised", as ultimately the victims of attacks are human beings, not machines or states.
- **Everyone has the right to secure communications:** Everyone has the right to use encryption, to remain anonymous, to use pseudonyms, and to be trained in digital security skills.
- **Security by design** (incl. privacy by design, no back-doors, etc.): Governments, nor anyone else, should have the right to arbitrarily build-in or exploit vulnerabilities in order to monitor or interfere with personal communications. *[4]*

Technology, services and the whole business environment is rapidly changing, leading to an exponential growth in cybersecurity issues. To curtail this, laws and norms need to be developed to secure the current and future cyberspace. New norms, complementing the few norms that currently exist, should help to protect cyberspace in terms of **encryption, back doors, and the removal of child pornography, hate speech, disinformation, and terrorist threats**. Though this is going to be a long process, progress on the various areas can take place simultaneously. *[10]*

Data & information security

A contributor stated that measures that reduce the security of information or that facilitate the misuse of secure information systems will inevitably **damage trust**, which in turn will **impede the ability of the technologies to achieve much broader beneficial societal impacts**.

Unfettered **strong encryption** to protect confidentiality and integrity of data and communications is essential for the protection of individuals, businesses and governments from malicious cyber activities.

Efforts by governments to restrict the use of strong encryption and/or to mandate **exceptional access mechanisms** such as "backdoors" or "key escrow schemes" — no matter how well-intentioned — will lead to the creation of vulnerabilities that would result in unforeseen effects as well as some predictable negative consequences:
- Malicious actors can use exceptional access mechanisms to exploit weakened systems or embedded vulnerabilities for nefarious purposes.
- Centralized key escrow schemes can be compromised, creating or increasing a risk of successful cyber-theft, cyber-espionage, cyber-attack, and cyber-terrorism.
- Exceptional access mechanisms increase the risk of malicious alterations to data, reduce trust in authenticity of data and might lead to decision-making errors and miscalculations.
- Efforts to constrain strong encryption or introduce key escrow schemes into consumer products can have long-term negative effects on the privacy, security and civil liberties of citizens. When these products are used worldwide, across jurisdictions, it may lead to illegal situations or conflicts with a country's standards and interests.
- Exceptional access mechanisms could hinder the ability of regulated companies to innovate and compete in the global market as customers may perceive their products as less trustworthy.

Law enforcement agencies have a range of **other investigative tools** to ensure access to systems and data, when warranted. Techniques include legal mechanisms for accessing data stored in plaintext on

corporate servers, targeted exploits on individual machines, forensic analysis of suspected computers, and compelling suspects to reveal keys or passwords. *[14]*

Sets of norms referred to by contributors

In order to ensure that all devices work on a regular basis contributors emphasized the importance of:

- Regularly run antivirus, antispyware and antimalware software; *[7] [11]*
- Regularly install patches that mitigate the impact of attacks, and remove vulnerabilities. *[11]*
- Avoiding that personal passwords or bank codes are stored on common and public devices. *[7]*

Contributors pointed to the work by the **Freedom Online Coalition, "An Internet Free and Secure"** *[2] [3] [4]* :

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**.
3. Cybersecurity- related laws, policies and practices should enhance the **security of persons online and offline**, taking into consideration the disproportionate threats faced by individuals and groups at risk.
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**.
7. Cybersecurity-related laws, policies and practices should **uphold and protect the stability and security of the Internet**, and should not undermine the integrity of infrastructure, hardware, software and services.
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.

Contributors referred to the **4 fundamental cybersecurity principles** defined by the **Cybersecurity Tech Accord**: *[5] [8]*

I. We will protect all of our customers and users everywhere.

II. We will oppose cyberattacks on innocent citizens and enterprises.
III. We will help empower users, customers and developers to strengthen cybersecurity protection.
IV. We will partner with each other and with likeminded groups to enhance cybersecurity.

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.

The field of cybersecurity norms is relatively unique in that the makeup of norms authoring organizations **reflects the diverse set of global stakeholders involved in the development of cyberspace** itself: academia, the technical community, industry, users, and governments have all contributed to the discussion around norms, from within their various and respective areas of expertise. **Industry has had a leading voice in the development of norms**, leveraging global visibility into the actions of harmful actors on the networks it operates to identify areas where international cooperation and agreement can be most impactful. *[1]*

One contributor mentioned that **very few organizations** stand up and promote specific cybersecurity norms within their field of work. Cybersecurity is considered as **overhead** in many organizations, with **business continuity dominating over cybersecurity**. A situation that will not change until people understand the intensity of cyber-attacks. *[11]*

A contributor specialized in cybersecurity and critical infrastructure mentioned the **lack of knowledge**, and the need to define common standards, in particular for the IoT or SCADA/ICS/PLC etc. A fundamental issue is the role of **firmware** and the lack of understanding of its importance among vendors and the end users. *[12]*

Organisations and initiatives promoting cybersecurity norms

The following organisations and initiatives that promote cybersecurity norms were mentioned in the contributions:

Progressive techie movement: An initiative where progressive technologists came together and talked about their rights and responsibilities. They do not deal specifically with cybersecurity, but they are concerned with end-users having the power to develop and control technology.[8] *[4]*

Digital security and safety training by APC members: APC's members are actively involved in building, promoting and providing training in digital security skills and tools. APC's Women's Rights Programme provides digital security training for women's rights and sexual rights activists and defenders.

[8] https://www.apc.org/en/news/progressive-techies-declare-their-rights-and-responsibilities

The Global Commission on the Stability of Cyberspace (GCSC) works on concrete norms and addresses both state and non-state actors. *[4] [5]*

Norms agreements and norms-related agreements reached by states at the **UNGGE**, **G20**, **G7**, **SCO**, **OSCE** and in other forums. *[5]*

The Digital Geneva Convention[9]: In 2017, Microsoft President Brad Smith issued a call for a Digital Geneva Convention, a proposed legally-binding agreement between nations about sensible limitations on state-sponsored cyberattacks against civilians and critical infrastructure in times of peace. *[5]*

Efforts of the Global Network Initiative, and specifically, more recently, of Microsoft to get industry to collaborate and commit to a culture of cybersecurity and defense. https://cybertechaccord.org/ *[4]*

Freedom Online Coalition: development of recommendations, for linking human rights and cybersecurity. (see question 2) *[4]*

The **NETmundial statement on cybersecurity**[10]**:** *[4]*

1. *Security and Stability*
    a. *It is necessary to strengthen international cooperation on topics such as jurisdiction and law enforcement assistance to promote cybersecurity and prevent cybercrime. Discussions about those frameworks should be held in a multistakeholder manner.*
    b. *Initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, private sector, civil society, academia and technical community. There are stakeholders that still need to become more involved with cybersecurity, for example, network operators and software developers.*
    c. *There is room for new forums and initiatives. However, they should not duplicate, but rather add to current structures. All stakeholders should aim to leverage from and improve these already existing cybersecurity organizations. The experience accumulated by several of them demonstrates that, in order to be effective, a cybersecurity initiative depends on cooperation among different stakeholders, and it cannot be achieved via a single organization or structure.*
2. *Mass and arbitrary surveillance undermines trust in the Internet and trust in the Internet governance ecosystem. Collection and processing of personal data by state and non-state actors should be conducted in accordance with international human rights law. More dialogue is needed on this topic at the international level using forums like the Human Rights Council and IGF, aiming to develop a common understanding on all the related aspects.*
3. *Capacity building and financing are key requirements to ensure that diverse stakeholders have an opportunity for more than nominal participation, but in fact gain the know-how and the resources for effective participation. Capacity building is important to support the emergence of true multistakeholder communities, especially in those regions where the participation of some stakeholder groups needs to be further strengthened.*

Country examples

A contributor described how in **India** legal provisions in the **Information Technology Act** (IT) aim to protect against cyber crime. The Indian CERT team has been working on areas of Cybersecurity, and other organisations, industry bodies and civil society organisations promote **best practices** to protect against cyber threats. The implementation of, and adherence to, these initiatives remains a **challenge**. The different initiatives are **working in silos**, and there's an urgent need bring them together under one umbrella and draft a unified set of norms, which today is missing. A **single set of norms** would be easier to implement and provide more benefit across different stakeholder communities. However, such a set of norms should be prepared by **involving all stakeholders** to assure a balanced and thought-out framework. *[6]*

[9] https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention
[10] http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

A contributor coming from a least developed country in Asia mentioned that in his country the general practice of cybersecurity culture is **something that is just evolving**. Cybersecurity auditing and compliance is limited within the **banking sector,** and gaining pace in other private sector organizations. There's a need for **more maturity and experience** in **adapting international standards**. Establishing international cybersecurity norms is an essential step in protecting national security in the modern world and maintaining trust in services provided online. [13]

Schools and organisations as promoters of norms

A contributor from Italy pointed out that **school are an important place for providing information on security**. Periodically, schools organize meetings with the communication police to enhance knowledge of recent laws and to report recent cyber crimes in order to make people aware of all the dangers which they are exposed to. *[7]*

Organizations with an information security department can stand up and promote specific cybersecurity norms. Global ICT companies, including Microsoft, have adopted policies and practices designed to alert users of popular online services when it appears that nation-states have targeted them. *[10]*

Governments, academia and civil society at the state and national level have put forward proposals, for example the Code of Conduct drafted by Shanghai Cooperation Organization (2015), or the agreement between the United States and China regarding cyber-enabled theft of intellectual property, law enforcement collaboration, and other cyber security measures. *[10]*

4. Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?

Norms restricting chemical and biological weapons - a useful example

There are useful parallels between discussions on chemical and biological weapons and discussions around cybersecurity. Lessons could be learned from the relative success of the use of norms in restricting the use of chemical and biological weapons. The successful creation, promotion, and adoption of norms restricting this devastating type of warfare has saved millions of lives and untold suffering. While there have been instances where norms have been broken, there is good evidence that most states abided by these norms, especially when they had confidence that other states would do so as well. Much like the cybersecurity landscape, the chemical and biological warfare arena also has dual-use technologies (lifesaving vaccines, for example) and a strong mix of academic, technical, and industry stakeholders supporting governments. *[1]*

One contributor mentions **simple rules** such as not opening any email, and above all any kind of attachment, from unknown senders, and stresses the importance of awareness of the risks online, in particular the risks children are exposed to. *[7]*

Inclusive and collaborative approaches to policy development

It was stated that **the norm to work with a multistakeholder approach** is very effective if different stakeholders can come together in a manner that creates trust and that gives everyone equal space to speak, and listen. As for example the African School on Internet Governance. *[4]* . **Openness and clarity** in a **multistakeholder** environment of consultation helps to create a better solution. *[13]*

Norms may evolve into law, depending inter alia on the political will of the relevant decision-makers and stakeholders. A discussion of norms – i.e. how the status quo should be, or what the relevant stakeholders should or should not be permitted to do – likely preceded the adoption of most conventions and legally-binding agreements.
In fact, such a discussion, elaboration and, ideally, adoption of norms can reasonably be described as a prerequisite for the establishment of binding legal agreements. It is in this push towards an ongoing discussion on how the status quo should be that norms are most beneficial. They are essential in facilitating an ongoing discussion and dialogue among stakeholders who may not (yet) be ready to discuss binding legal agreements. *[5]*

A contributor referred to **Chile** as an example of positive collaboration between a national government and civil society on cybersecurity legislation. Rather than criticising everything the government was doing, civil society worked with the government and provided alternatives, finding ways in which they could obtain better cybersecurity measures that respect human rights. Through this, the civil society developed its capacity and helped the government to better understand human rights concerns. *[4]*

A contributor recommends that existing cyber security measures that are already implemented in individual organisations are identified and brought together in a framework that then can be applied across all organizations. Strong working teams should be formed to improve security. *[10]*

A contributor flagged that a program should be launched to deal with potential security issues related to the use of firmware in Critical Infrastructures. *[12]*

Importance of effective enforcement

One contribution emphasizes the importance of **having effective and enforced processes and policies**. Many organizations are getting focused on building processes and policies, but no enforcement is in place. Examples show that where processes and policies are approved and enforced by top management have been very effective at improving security. *[11]*
Another contributor notes that AUPs, ToSs and ASPs are adequate and potentially effective, but missing enforcement by their administrators. *[9]*

National Frameworks and examples

- The Framework for Improving Critical Infrastructure Cybersecurity, developed by the U.S. National Institute of Standards and Technology ("NIST Framework"), is becoming an important best practice norm and has therefore quickly gained broad adoption across the world, or inspired similar frameworks in other countries:
    - The Italian cybersecurity framework (2015), which focuses on small and medium sized enterprises, largely borrows the NIST Framework.

    - The Australian Securities and Investments Commission (ASIC) in 2015 issued Report 429 Cyber resilience: Health check (REP 429),which encouraged businesses to consider using the NIST Cybersecurity Framework to assess and mitigate their cyber risks or to stocktake their cyber risk management practices.
    - The International Standards Organization (ISO) has recently approved work on a technical report on "Cybersecurity and ISO and IEC Standards", which seeks to adapt the NIST Cybersecurity Framework to the international environment. *[8]*

- The cybersecurity **norms developed by RBI (Reserve Bank of India)** regarding digital transactions have proved to be successful to some extent. Recently the Department of Information Technology in India has been working closely with RBI to further enhance the security levels to defend cyber risks. It has created an Audit Management Application portal to handle various supervisory functions of the cybersecurity and information technology examination cell in the Reserve Bank and to fully automate monitoring of returns. It was envisaged to facilitate consistency and efficiency of the offsite monitoring mechanism. *[10]*

- On 6 February 2018, the international 'Safer Internet Day', the **European Union Agency for Network and Information Security (ENISA)** published a report providing organizations with practical tools and guidance to develop and maintain an internal cybersecurity culture. The report identifies good practices from the organizations that have already implemented cybersecurity culture programmes. These tools can be used for enhancing the cybersecurity levels of other organisations. *[10]*

5. Do you have examples of norms that have failed (they have not seen widespread adherence), or had have adverse effects (living up to the norm led to other issues)?

Factors influencing the failure

Norms are not always successful. Indeed, Finnemore (2017)[11] suggests that failure may be the most likely outcome for any given norm. One key element that could precipitate the failure of a norm is the **lack of adaptability to meet new technological, cultural, and political realities**. This could cause actors to abandon the norm out of convenience more than malicious intent and may lead to unintended consequences. It is therefore imperative that the hard work that goes in to development of norms create **flexible norms that can be evolved over time**. *[1]*

A contributor warns that while trying to build a cybersecurity culture, people create a **culture of fear** - e.g. by highlighting the damage done by cyber-attacks - which has adverse effects and moves people away. *[11]*

[11] Finnemore M (2017), "Cybersecurity and the Concept of Norms," Carnegie Endowment for International Peace. Available at: http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870

While it could be argued that the norms-building effort for cybersecurity has failed, it is more likely that it is going through the **acceptance building phase**, where normative standards become established. While a lengthy acceptance building phase might be common in traditional environments, it represents a significant challenge in the fast-moving online environment. The lack of action is likely to discourage norms entrepreneurs from putting forward new rules of the road, as well as allowing for further escalation of tensions in cyberspace. *[8]*

Despite the development of new norms for cyberspace in various forums representing different stakeholder groups and state organizations, **no single set of international cybersecurity norms have been recognized or adhered to by nation states**. In the absence of recognized norms, the escalating instability of cyberspace continues unabated. Perhaps the most recent examples of this escalating behavior are the Russian cyberattacks against political and civil society institutions within the US in August 2018. *[5]*
It is clear that the international cybersecurity norms that have been proposed and agreed to so far have **not been adhered to by nation states**, at least not consistently. While there are examples that have been promoted as successes, for instance the supposed reduction of cyber espionage in the aftermath of the China-US cybersecurity agreement, successes like that have been few and far between. *[8]*

The **Implementation of norms and their adherence** is a major concern. Making the process too complicated or not explaining the norms clearly and lucidly to the people who would be implementing or abiding by the norm at times have adverse effects as people take it as a **burden** and do not follow it wholeheartedly. *[6]*

The **norm of multistakeholder approaches** is every unevenly adopted. For example, the participation from both international and India-based civil society organisations in the Global Conference on Cybersecurity, held in Delhi in 2017, was severely restricted. *[4]*

The **lower and developing nations are just working their way.** In most of the countries the overall process of standardization has a huge challenge of multistakeholderism where cybersecurity is one of the hottest topics that comes up. New standards and norms are also coming up which needs to be guided by better core values. *[13]*

Needs & suggested improvements
What is needed now is the **consolidation, interpretation, and universal recognition** of the norms that have already been agreed to at the regional and multilateral level by governments around the world. This consolidation would effectively set the baseline for future and ongoing discussion on, and negotiations of, the issue. With a salient list of internationally-recognized cybersecurity norms, endorsed by a multistakeholder coalition including national governments, the international discourse could then turn to the promotion of the norms and to accountability efforts. *[5]*

Examples of incomplete norms or reverse effects
In June 2014, the **African Union Convention on Cyber Security and Protection of Personal Data** text was finalised. Some AU countries have ratified the Convention. The contribution highlights some ways in which the Convention text could have been improved and its potential negative impacts:

- Poor definitions for content restrictions: “child pornography” restrictions were not well defined and overbroad. Conversely, protections for persons against incitement to violence failed to include LGBT.
- “...the Convention fails to put safeguards into the sharing of information between companies and governments” and does not adequately limit the authority of cybersecurity regulators.

Beyond potential negative impacts, there are aspects of the Convention that are of far more immediate concern:

- The exception to the requirement of user consent in order to process personal data when in “performance of a task carried out in the public interest or in the exercise of official authority” is dangerous.
- Use of a computer to “insult” someone is banned, yet the term is never defined. In any case, this has the potential to criminalise legitimate speech as defined in international human rights law.
- Technologists and journalists are at increased risk of their work being criminalised due to overly broad definitions of “computer fraud” and “fraudulently obtained data” in cybercrime provisions. *[2]*

The failure of the **Group of Governmental Experts (GGE) of Information Security** convened by the United Nations in 2016-2017 to arrive at a consensus outcome report during its last round of deliberations, is mentioned by one contributor as an example that indicates the importance of devising effective norms for cybersecurity. *[10]*

Constructing a new norm is difficult and not an easy task. Sometimes conflicts exist or compromises exist. This may lead to the failure or success of any upcoming norms. If the norm is perceived as a burden or obstacle, it will likely be ignored by the employees. It is important to examine the current cybersecurity culture with regard to strengths and weaknesses to avoid the adverse effects. *[10]*

Students often take video during lessons and even all the sanctions they have been given, they continue to make video for uploading them on the net. Notwithstanding all the recommendations each teacher suggested, they aren’t able to get rid of that bad habit. *[7]*

One contributor notes that no ISP, Registrar or RIR obeys AUPs, ToSs, ASPs and Codes of Conduct that are on their websites. The same contributor adds that the current GDPR Directive protects the companies rather than the population. *[9]*

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

While the development of cybersecurity norms is still relatively nascent (with the first truly global norms having appeared within the last 5 years), it is **too early to tell whether the implementation of a given norm has been successful.** Norms generally take long periods of time to achieve relative adherence, and violations of norms in other areas do occur, although rarely. We appear to still be in

the "**entrepreneurial" phase** of norms development as defined by Finnemore and Sikkink (2007)[12] and mass adoption has not yet materialized. However, the development of norms in the global context is important, as the security threats to the stability of the Internet are also global. There are, however, useful opportunities for the adoption of norms in the **regional context.** Singapore's decision to promote the cyber norms agreed to within the UN Group of Governmental Experts (UNGGE) in 2015 within the context of the Association of South East Asian Nations (ASEAN) is encouraging and hopefully other countries in the region will support this initiative. In addition, the development of norms must be accompanied by the development of **confidence-building measures** and **capacity-building programs** to help states and other relevant actors understand how the norm is being adhered to by other actors and to internalize the norm into the actors' own processes and policies. This will be key to ensure national cybersecurity strategies are aligned with the values and objectives of the wider cybersecurity community, which will contribute to creating a safer cyberspace for all. *[1]*

Policies are implemented, whereas norms are standards that are set with the intention of adoption or influence for policy making. *[2]*

All norms, irrespective of the focus area they have emerged in, have one thing in common. Their **acceptance took time**, unless they have emerged in a response to a catastrophic event. This is particularly true as it relates to weapons frameworks, an area which cybersecurity is often compared with. Norms adoption and implementation often requires nation-state actors to give up a strategic advantage for the common good, which is a difficult hill to climb under any circumstances. *[8]*

In the absence of a catastrophic event, the role of civil society has always been colossal. **Norms implementation requires a watchdog**, formal or informal, that can call out positive actions by nation-states and highlight bad behavior. Today this happens too rarely, and when it does, the actions called out are rarely linked with established norms, such as the ones adopted by the UNGGE. *[8]*

While attribution in cyberspace is difficult, it is not impossible, and it is important that investments in this space continue. Much can be done by encouraging governments to make their cyberwarfare doctrines public, encouraging transparency and investment in implementation of risk-management policies. *[8]*

Some norms **emerge spontaneously** without any particular actor having any particular intent and then become entrenched through habit. In any group that interacts regularly, norms develop simply through expectations shaped by repeated behavior. Much of the foundational engineering of the Internet involves this kind of path-dependent norm development.The most effective method of implementing cybersecurity norms would be through a **public dialogue process** like a national Internet governance forum and other policy development process which provide a better platform and situation of understanding and mitigation of the problems and challenges. Another way can be understanding the problem or challenge of cybersecurity and doing a proper research in opening up the process for dialogue in a multistakeholder environment for policy development process and can create better solution. During the Wanna Cry virus attack various collaborations emerged creating a proper cybersecurity norm and mitigating the problem. *[13]*

[12] Finnemore M and Sikkink K, (2007), "International Norm Dynamics and Political Change," International Organization, Vol. 52, No. 4, International Organization at Fifty: Exploration and Contestation in the Study of World Politics. (Autumn, 1998), pp. 887-917. Available at: http://links.jstor.org/sici?sici=0020-8183%28199823%2952%3A4%3C887%3AINDAPC%3E2.0.CO%3B2-M

The following are required of a global or regional initiative to implement human rights oriented norms and standards:

1. A fundamental rethink of the dominant rights versus security paradigm and **recognition that human rights and cybersecurity are mutually reinforcing and interdependent**
2. **Sustained and deep engagement in international policy** and in particular cybersecurity dialogues at key international forums to promote such norms.
3. **Case study development** demonstrating the beneficial effects of people-centric cybersecurity policy.
4. **Consistent evaluation** of cybersecurity policies and strategies using a human security framework, such as indicators based on the above norms.
5. **Multi-stakeholder initiatives** that combine these elements are an absolute necessity. *[3]*

Effective methods to demand ethical behaviour from Internet providers are needed in order to reduce the negative effects to the end users of the internet. *[9]*

Awareness & Enforcement

Creating awareness effectively contributes to implementing cybersecurity norms. People need to know why it is important to follow a norm and the consequences if the norm is not respected. The implications of not following the norms worldwide should be well communicated. At the same time, management teams should emphasize on cybersecurity as well. The **enforcement** has to be from the top. *[11]*

For voluntary norms that have been developed for cyberspace to meaningfully curb irresponsible state behavior, they must be more widely recognized, respected and insisted upon by nations, industry and civil society alike. When norms are violated, such **violations must be clearly identified and denounced** by all who were impacted. Attacks such as NotPetya, which so significantly damaged companies including Maersk and FedEx, should not be accepted as the new normal but rather denounced as violations of international norms in cyberspace. Such denouncements must be prolific and continuous, and demand an improvement of the status quo. *[5]*

The challenge of reinforcing cyber norms is exasperated by the difficulties associated with **accountability following cyberattacks**. In the wake of cyber incidents today, perpetrators are rarely ever accused of malfeasance, and never truly held accountable for their actions. When attribution does occur, it is done by individual states or small coalitions of like-minded nations and based on investigations that are never made public. Unsurprisingly, this process results in denials and is without any meaningful accountability.What is needed is an **independent, multistakeholder body** – with international credibility – to conduct impartial forensics following cyberattacks and to provide evidence to the international community free of any semblance of bias. *[5]*

Firstly, there is a **need for in-depth research** on the subject. Secondly, it is important to create an **awareness among all stakeholder groups** –government, business, civil society on the threats of cyber security; the importance of having common cybersecurity norms; advantages of following norms and the implications of not adhering to them. *[6]*

Training and capacity building will help to make communities aware and adopt norms. Simultaneously, IGF and the NRIs, which are open platforms, should encourage more discussions on

best practices and ways to address concerns of implementing cybersecurity norms, which will be of immense benefit to the community. *[6]*

Implementing cybersecurity norms is something related with **specific technical competencies** but lot of **tips come from ordinary usage**. *[7]*

i) Carry out the **research** regarding cybersecurity.
ii) Collect **technical reports** from the cloud server and academia as well as journal publications regarding cybersecurity.
iii) **Cybersecurity culture programs** can be initiated among the organizations which want to adapt the change and to become most successful.
iv) Through **awareness programs**, webinars, brainstorming and training sessions.
v) **Cybersecurity frameworks** can be developed. *[10]*

Examples

- The **African Union Cybersecurity and Data Protection Convention** was an important step to setting norms for African states. The subsequent adoption of the Convention by other African states is working well as some countries have ratified the convention or are slated to do so. And some states have already implemented their own conventions, strategies, policies or legislation. However, African states' adoption of cybersecurity and, in particular, data protection laws is happening at a very slow pace. *[2]*

- The implementation of **cybersecurity and data protection legislations at the national level in Africa** is positive in countries where policy decisions, design and implementation considers input and advice from all stakeholders, in particular when civil society is included at each step. *[2]*

- There are examples where at a local or national level, industry, law enforcement and rights advocates have collaborated in developing policy and regulation. This might not qualify as implementation. Most of the contributor's experience is related to **digital security and implementing measures to ensure the security of users particularly in vulnerable communities**, e.g. women's human rights defenders. *[4]*

- The introduction of the **NIS directive** at EU level will provide important legal framework but is too general. *[12]*

7. Within your country, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

General comments acknowledging a cybersecurity divide

The Digital Security Divide is quite evident. The divide can be clearly seen between **developed and developing nations**, **literacy and socio-economic levels**. The digital security divide is higher in developing nations, people with lower literacy levels or coming from lower socio-economic strata. This can be attributed to the lack of training or awareness of online safety. *[6]*

With the growth and advancement of the technology, a new form of digital divide is growing between the security 'haves' and the 'have nots'; the **digital security divide is growing**. *[13]*

The Digital Security Divide is not the sole **responsibility** of the people or the country but both. *[10]*

There is no common security framework. The U.S. use its approach, the EU doesn't have a common standard, and China is developing its requirements. *[12]*

Contributions mentioning a Cybersecurity divide between nations

More than "better" or "worse" cybersecurity, the **digital divide between nations** results in different challenges for countries based on their respective states of digital transformation as well as their unique sociopolitical and geopolitical contexts. **Nations whose citizens and businesses are coming online today are entering a sophisticated cybersecurity environment both in terms of threats and opportunities.** While they face a steep learning curve in navigating dangers online, they also have the potential to leverage new technologies to leapfrog the challenges that plagued previous generations of internet users. *[5]*

Countries coming online today can benefit from **applying international best practices**, such as the Budapest Convention on Cybercrime,and the NIST framework, to avoid unnecessary pitfalls. (...) Unfortunately, nations too often still start from scratch when it comes to cyber policy – a process that can take years during which they could otherwise be working on further improving their national cybersecurity posture and culture. *[5]*

Contributions mentioning a cybersecurity divide between people / users

One contributor describes that some users have better cybersecurity than others, a difference both **between people and countries**. For people the main driver of the divide is people's mindset, attitude and beliefs towards cybersecurity. For countries the main driver of the divide is the susceptibility of getting attacked by other countries. Also the number of cyber-attacks and the damage done plays a role. *[11]*

In lower economies **users who lack the skills, knowledge and resources are vulnerable** to cybercrime and hacking. Addressing this digital security divide will be critical to realizing the full potential of the future Internet. *[13]*

The divide is partly because of **malicious actors weakening security for certain people, groups, or countries**, for example government hacking, exploitation of vulnerabilities, weak security measures employed when handling sensitive personal data, etc. Dissidents, journalists, women, people who face discrimination based on sexual orientation or gender identity (SOGIE) and others are often targeted by malicious actors and therefore suffer from lack of security online. *[4]*

Within an organization there's a divide depending on the level of understanding of security concerns. For example, a security professional will be more conscious of security issues, whereas a member of the sales team may not be quite conscious/aware about security issues. *[6]*

Factors influencing the cybersecurity divide

Lack of data protection laws to require protection of personal data and notice of security breaches. *[4]*

There's a **lack of awareness of risks, education and digital security skills.** More capacity building, training and promotion of best practices and norms can help to reduce the digital security divide. *[4] [6]*

The gap between users who are secure when they use digital communications and those who are insecure is not due to the failures or triumphs or individual users. The gap is due to the actors, largely from the private sector, responsible for positive or negative impacts on user data and security, and whether or not the state has taken the initiative to properly regulate those actors. *[2]*

Governments are not investing in cybersecurity awareness and capacity building, companies are not implementing privacy by design, so it's not fair to blame the user for not having the skills necessary. *[4]*

In some countries, **policy decisions can exacerbate these security divides**: forcing personal data to be localized in less secure systems that can't take advantage of the state of the art in cybersecurity, for example, can mean that users in some countries are forced to exist with a less-secure Internet experience, which can reduce their adoption of digital technology due to a lack of trust. *[1]*

Decisions by national governments that do not consider the global nature of cyberspace or take advantage of the global community's knowledge, expertise and development of best practices on cybersecurity can put users at risk. The same goes for governments that adopt policies that do not foster collaboration between stakeholders both within and across their borders in terms of digital skills training and cybersecurity awareness raising. *[1]*

Annexe: Report of the BPF Cybersecurity session at the IGF 2018

IGF 2018 Best Practice Forum on Cybersecurity

Wednesday 14th Nov, 10:10-11:40 CET, Salle XII
Paris, France

Co-moderators: **Markus Kummer,** Internet governance & policy consultant
Kaja Ciglic, Microsoft

Format:

1. Introduction by the co-moderators
2. Run-through of this year's BPF output
   Wim Degezelle, IGF consultant BPF Cybersecurity
3. Interventions by a selection of the contributors to the 2018 BPF Cybersecurity output:
   Alexander Klimburg, representing the contribution from the Global Commission on the Stability of Cyberspace (GCSC)
   Ephraim Percy Kenyanito, representing the contribution from ARTICLE 19 Eastern Africa
   Saleela Salahuddin, Facebook representing the contribution from the Cybersecurity Tech Accord
4. Round-table discussion open to all participants (50 mins)

Theme: Cybersecurity, Trust and Privacy

Transcript / recording **:**
https://www.intgovforum.org/multilingual/content/igf-2018-day-3-salle-xii-bpf-cybersecurity

Report:

Session Type (Workshop, Open Forum, etc.): Best Practice Forum
Title: 2018 Best Practices Forum on Cybersecurity
Date & Time: Wednesday 14th Nov, 10:10-11:40
Organizer(s): Markus Kummer, Internet governance & policy consultant (Technical Community) and Ben Wallis, Microsoft (Private Sector)
Moderators: Markus Kummer, Internet governance & policy consultant (Technical Community) and Kaja Ciglic, Microsoft (Private Sector)
Rapporteur/Notetaker: Ben Wallis, Microsoft
List of speakers and their institutional affiliations: Mr. Wim Degezelle (IGF Consultant BPF Cybersecurity), Mr. Louk Faesen (Global Commission on the Stability of Cyberspace (GCSC) - Technical Community), Mr. Ephraim Percy Kenyanito (ARTICLE 19 Eastern Africa - Civil Society), Ms. Saleela Salahuddin (Facebook / Cybersecurity Tech Accord - Private Sector)
Theme (as listed here)**:** Cybersecurity, Trust and Privacy
Subtheme (as listed here)**:** Cybersecurity best practices

Key messages of the discussion

The importance of norms as a mechanism in cybersecurity for state and non-state actors to agree on a responsible way to behave in cyberspace, given that the speed of legislation often struggles to keep up with the pace of changes in the sphere of cybersecurity.

The importance of multi-stakeholderism – threats to cybersecurity impact governments, private companies and people. There are a number of helpful norms, on different aspects and from various parts of the world, but more needs to be done to involve non-state stakeholders in the development and implementation of norms.

Cybersecurity norms and laws should be respectful of human rights, and not stray into areas such as freedom of expression and control of content online. It is important to separate the security of the infrastructure, which this BPF is focused on, from questions of content shared online.

Summary of the discussion

The work of 2018 BPF identified the norms that exist and any best practices that can be learnt; and then looking into the question of a digital security divide in which some sets of users have better cybersecurity protections than others. It recognises that norms have become more important as a mechanism for state and non-state actors to agree on a responsible way to behave in cyberspace, partly because traditional law-making is generally not able to keep pace with the evolution of online security threats. It found that there are a great variety of norms, varying from the culture of cybersecurity within a company to behaviours of end users, including an example of a teacher in the classroom. However, norms are often developed in relatively small and close communities which focus on their areas of expertise and do not involve or communicate with others. And they are often developed by a specific group of stakeholders or countries which can make it difficult to transfer them to a multistakeholder environment. The 2018 BPF output can be seen as valuable in raising visibility of norms developed outside the intergovernmental realm, which governments are sometimes less aware of.

There are some positive recent examples of new norms being developed, including Geneva Dialogues in Switzerland, an ASEAN commitment on norms, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) and the framework developed by the US standards body, NIST. But many norms are developed between states or within the private sector. When norms are developed, it is important to find ways to bring in technical expertise and allow for the involvement of stakeholders. The November 2018 Paris Call is an encouraging exception, with almost 400 signatories coming from across governments, the private sector, the technical community and civil society, and a focus on working together with different stakeholders to tackle these challenges.

An illustrative example is the Global Commission on the Stability of Cyberspace (GCSC). It has a mandate very much focused on developing and implementing norms, and has recently

adopted the Singapore Norm Package, providing six further norms to the two previously agreed, and with the express purpose of having them adopted by public and private sector actors towards an architecture to improve international security and stability in cyberspace. However, the GCSC is a discussion just between governments, and only 25 of them. It could benefit from the expertise and knowledge of stakeholders, conscious that the technical community and civil society manages much of the Internet and the private sector owns most of the critical infrastructure.

A major example of private sector efforts to develop norms is the Cyber Tech Accord which has brought together over 60 large and small companies representing network operators, software developers, social media companies and cybersecurity researchers. Its work is based around some central norms – to protect all customers, to oppose cyber-attacks on innocent citizens and enterprises, and to help empower users, customers, and developers to strengthen cybersecurity protection. Beyond developing high-level norms, it also develops capacity among its members through sharing technical information and providing training. In taking responsibility for its role, a particularly important element for the private sector is the principle of security by design, which should be enshrined in many of these norms.

Policy recommendations or suggestions regarding the way forward/potential next steps

It is important to separate the security of the infrastructure, which this BPF is focused on, from questions of content shared online. Issues such as freedom of expression, data protection, intellectual property have their own separate legal frameworks and should not be taken within cybersecurity laws or norms. One panellist spoke of cybersecurity laws being adopted which also bring in non-cybersecurity measures, such as prohibiting the sharing of information over the Internet by public officials or making it illegal to question official statistics.

Capacity building is needed in terms of both financial resources. More partnerships would be an important way to help achieve this, helping to get experts in various regional levels and at the ground level to spread expertise and norms into all parts of the world.

In the discussion, it was suggested to think about the various steps required to have norms in place. Between designing norms and implementing them, there is an intermediate step which one panellist described as “norm authorisation”. This relates to identifying which kinds of bodies, beyond governments, could take on the authority for driving the implementation of norms, and could also extend to providing some kind of accountability for attributing non-compliance with norms and creating pressure which can help the norm become accepted over time. The media can also play a role in shedding light on exploitations and subversion of cybersecurity norms or drawing attention to best practices.

What ideas surfaced in the discussion with respect to how the IGF ecosystem might make progress on this issue?

The IGF does not have a mandate to develop norms or to be any kind of authorisation body related to norms. However, there could be a role for the IGF to continue its intersessional

work on cybersecurity by contributing to developing a narrative, e.g. what do we mean of this norm, and what should be done or not be done to essentially illustrate what could be done going forward. It could also be interesting to look at how the IGF could take forward ideas with the Paris Call for Trust and Security in Cyberspace.

Estimated total number of participants. About 65
Estimated total number of women and gender-variant individuals present. About 30
Gender issues discussed at the session? The session did not discuss cybersecurity in the context of gender; only cybersecurity as it relates to society as a whole.
