IGF 2018

Best Practices Forum on Cybersecurity

Cybersecurity Culture, Norms and Values

Background paper to the IGF Best Practices Forum on Cybersecurity.

Editor:
Maarten Van Horenbeeck, BPF Lead Expert (maarten@first.org)

Key contributors:
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

Many thanks to all participants of the IGF Best Practices Forum on Cybersecurity, led by Markus Kummer and Bem Wallis, and UN consultant Wim Degezelle. We are an open, multi-stakeholder group conducted as an intersessional activity of the Internet Governance Forum. Join us at https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1

Table of contents

Introduction to the Best Practices Forum on Cybersecurity

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 Practices 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 is focusing on the culture, norms and values in cybersecurity. The plan of action for the Best Practices Forum is:

- 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 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.

This document was established with support from participants in the Best Practices Forum, and serves as an introduction to the wider area.

It helps establish where gaps exist, and serves as background reading to anyone interested in responding to our Call for Input. The outcome document of the BPF will substantively change and build on this document based on the input received by the wider group.

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[1] and civil society, operating “in their respective roles” through “rough consensus and running code”[2]. 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 nonstate 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 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.

[1] 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.

[2] 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).

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[3] 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 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[4] decision-making process is also present in other technical settings.

[3] 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.

[4] 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.

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.

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