IGF 2018
Best Practice Forum on Cybersecurity

Cybersecurity Culture, Norms and Values

BPF output part II

Summary report of the public contributions to the IGF BPF on Cybersecurity

Draft Report 1 November 2018

Table of contents

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. 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**.

Cybersecurity Culture, Norms and Values

Norms have become a very important mechanism for states and non-state actors to agree on responsible behaviour in cyberspace. There are numerous initiatives under way in this regard, but with limited exceptions, such as the Global Conference on Cyberspace (GCCS) and the Global Commission on the Stability of Cyberspace (GCSC), most of these norms discussions happen in inter-state forums, and they do not always provide an open and inclusive mechanism for non-state actors to participate and to contribute. The Best Practices Forum is taking a multi-stakeholder view on the development of norms, both within and between participants of each IGF stakeholder community.

The BPF on Cybersecurity produced a Background document that serves as introduction to the wider area of culture, norms and values in cybersecurity. This document is available on the IGF website and is together with the summary of contributions the output of the 2018 BPF on Cybersecurity.

Cybersecurity Culture, Norms and Values - BPF Background paper
http://www.intgovforum.org/multilingual/filedepot_download/3405/1294

Methodology

The BPF Background paper was established with support from participants in the BPF Cybersecurity. Its main contributors are acknowledged in the document. The background document was published on the IGF website together with the BPF's *Public call for contributions* to provide an introduction to the wider area of culture, norms and values in cybersecurity.

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 the Summary report.

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 Report

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.

BPF Call for Contributions - 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?

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.[1] *[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.

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

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

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[2]: 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**[3]**:** *[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

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

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]*

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)[4] 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]*

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]*

[4] 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

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)[5] 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]*

[5] 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

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]*

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]*