2016 Internet Governance Forum (IGF) Best Practice Forum (BPF) on Cybersecurity

'Building Confidence and Security in the use of Information and Communications Technologies (ICTs) through Enhanced Cooperation and Collaboration'

Part I: Framing the 2016 IGF Best Practice Forum (BPF) on Cybersecurity Multistakeholder Dialogue

The report[1] of the IGF 2015 Main Session on Enhancing Cybersecurity and Building Digital Trust held on 12 November 2015 stated the following:

> *"The general consensus coming from the session was that cybersecurity is everyone's problem and everyone should be aware and understand that the cyber world is a potential unsafe place. 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.*
>
> *There were calls for further multistakeholder participation in the tackling of cyber-crime. Session panellists agreed that the IGF, including National and Regional IGFs (NRIs), has proven to be a good collaborative multistakeholder process for cybersecurity, but still needs to reach out to get missing parties around the table. The involvement of the government, private sector, civil society and other stakeholders in handling cybersecurity was stressed as fundamental in terms of sharing best practices, sharing results of critical assessments and identifying globally accepted standards of cybersecurity. All stakeholders must understand, respect and trust each other's expertise and competences."*

Building on this report and emerging demand from the IGF community for an additional multistakeholder dialogue platform to discuss issues related to cybersecurity, during the IGF Open Consultations and MAG meeting from 4-6 April 2016[2], there was agreement that a 2016 IGF BPF would be carried out on a cybersecurity related topic, building upon the previous work of the CSIRTS and SPAM BPFs[3]. The MAG meeting also acknowledged that the WSIS +10 review process had produced an outcome document with a strong focus on "building confidence and security in the use of information and communications technologies", making an IGF BPF related to cybersecurity even more relevant and timely.

---

[1] http://www.intgovforum.org/cms/documents/igf-meeting/igf-2015-joao-pessoa/igf2015-reports/609-igf2015enhancing-cybersecurity-and-building-digital-trust

[2] http://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/magmeetings/732-summary-igf-1st-oc-and-mag-meeting-4-6aprilfinal

[3] http://www.intgovforum.org/cms/best-practice-forums/2015-best-practice-forum-outputs

While reviewing the outcomes of both the IGF Spam[4] and CSIRT[5] Best Practices Forums (BPFs) held in 2014 and 2015, there was an emerging consensus amongst the community that the 2016 cybersecurity BPF would benefit from addressing cooperation and collaboration between stakeholder groups as a central topic[6]. It was said during an initial Virtual meeting for the BPF that one of the lessons learned during the work on the IGF BPF on CSIRTS was that it attracted a mostly engineers working on technical issues. The BPF group found that while CSIRT teams in most cases find agreement within their own communities, there were significant communication issues when engaging with other stakeholder groups, in particular policy makers, civil society, but also law enforcement and even industry.

The community also expressed that all stakeholders would benefit from having a multistakeholder discussion, including each of the major IGF stakeholder groups, on how to engage and communicate with each other on cybersecurity issues. There was also a feeling that this would be uniquely fit for an IGF BPF and that the work carried out in 2016 should not be seen in isolation, but should rather be seen in a long-term perspective and that capacity building would be an integral component for the work. End users, law enforcement agencies, policymakers, and all of the other range of actors involved in cybersecurity should be invited to get involved in the work on an ongoing basis. It was also noted by a group of BPF participants that focusing on cooperation and collaboration would support the Internet Governance Principles laid out at the NETmundial Statement[7], that recognize that "Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders".

It was also emphasized during the first few BPF Cybersecurity virtual meetings[8] that to many today, the word “cybersecurity” is often loaded with context, and many organizations associate it with government decision making, or commercial security solutions. Within the IGF, it was said, there is an opportunity to redefine cybersecurity as a common goal between all stakeholders, and to work towards finding a common understanding what productive cooperation and collaboration might look like.

In a contribution to the BPF from Mr. David Strudwick[9] it was suggested that cybersecurity ‘situational awareness’ could also be a complementary topic for the BPF to explore in its work. The contribution defined cybersecurity situational awareness as “Both knowing and influencing combined risks and applied mitigations”; or in more detail, “The resulting sensitivity to a local risk state that arises from clearly establishing vulnerabilities and threats and the commensurate measures to mitigate such threats, while supporting and maintaining the confidentiality, integrity, availability and non-repudiation of information within integrated computing and communications systems.”

---

[4] http://www.intgovforum.org/multilingual/content/2015-best-practice-forum-outputs

[5] http://www.intgovforum.org/multilingual/content/2015-best-practice-forum-outputs

[6] See 2016 IGF BPF Cybersecurity Virtual Meeting Summary’s from May-August 2016: http://www.intgovforum.org/cms/best-practice-forums/bpf-cybersecurity

[7] http://netmundial.br/netmundial-multistakeholder-statement/

[8] Initial Contributions/Ideas/Suggestions received via emails on BPF Cybersecurity Mailing List: Proposal from: Andrew Cormack, *Jisc*Adli Wahid, *FIRST*, Cristine Hoepers, *CERT.br/NIC.br* Peter Cassidy, *Anti-Phishing Working Group (APWG)*, Maarten Van Horenbeeck, *FIRST*, Serge Droz, *FIRST*; Neil Schwartzman; Jerome Athias; James Gannon; Serge Droz; Marilyn Cade; David Strudwick; Michael Ilishebo; Alejandro Pisanty; Wout DeNatris; Cheryl Miller; Nick Shorey; Richard Leaning and more.

[9] http://www.intgovforum.org/cms/documents/best-practice-forums/881-cdd-igf-proposal-20160617

The proposal suggested that the IGF BPF Cybersecurity dialogue space could work towards helping to "establish a common international *scaffolding* and development of emergent best practice supporting *security situational awareness*, with the intention to achieve globally applicable common policy towards increasing technical *capabilities,* reduction in *vulnerabilities* and the exertion of positive *influence* engendering increased *confidence* in the operation of underlying information technologies, on which the Internet relies."

Two contributions[10] from the Internet Society (ISOC) to the BPF also emphasized the importance of cooperation and a collaborative approach in multistakeholder efforts to build confidence, user trust and security in the use of Information and Communications Technologies (ICTs). In ISOC's Executive Summary of their Policy Framework for an Open and Trusted Internet, they state:

> *"Large scale data breaches, uncertainties about how our data is being used, cybercrime, surveillance and other online threats are impacting Internet users' trust, how they use the Internet, and hindering Internet adoption. Policymakers are facing an important challenge today: How to fully embrace the digital revolution while, at the same time, ensuring the safety and security of their citizens. The Internet Society believes the Internet needs a solid foundation in trust to achieve its full potential. Trust is a cornerstone for all successful connectivity strategies, in developing and developed countries alike. This can only be achieved through collective responsibility and collaboration."*

ISOC's collaborative security approach to tackling Internet security issues further emphasizes that the Internet itself was built through voluntary cooperation and collaboration and cooperation and collaboration remain the essential factors for the Internet's prosperity and potential. Further, the approach emphasizes that everyone has a collective responsibility for the security of the Internet and multistakeholder cross-border collaboration is an essential component.

Framing working definition(s) of Cybersecurity:

http://policyreview.info/articles/analysis/what-we-talk-about-when-we-talk-about-cybersecurity-security-internet-governance

"The term 'Cybersecurity' is used for many different purposes. Many professionals consider that it is particularly valuable to use all terms that include 'security' sparingly, and then more as shorthand for sound risk management.

It is valuable to distinguish between national security, public security, enterprise security and personal security. Further, much clarity arises when discussions have a clear starting point in signalling what assets are being protected against which risks, even if in a broad picture. thus, cybersecurity as national security encompasses, attacks that may impede the functioning of a society as a whole and threaten a nation's sovereignty or survivability; enterprise security includes separately its operational infrastructure and its intellectual property; for an NGO oriented to the defence of human rights, cybersecurity may encompass the confidentiality of its membership, sources of information and activities; threats to its reputation, and the drowning of its discourse in social media; for the average citizen, threats are mostly against life and

[10] Internet Society (ISOC): *A policy framework for an open and trusted Internet* – http://www.Internetsociety.org/doc/policy-framework-open-and-trusted-Internet *and Collaborative security approach to tackling Internet security* issues: http://www.Internetsociety.org/collaborativesecurity

limb, reputation, and economic assets. The best practices in cybersecurity will ensue from a proper, proportionate analysis of risks, costs and benefits for each case and the risk-management disciplines that can best prevent and mitigate attacks."

From Kush Singh:

"In my opinion I find Cyber Security as a much generalized term. To most of us it doesn't mean much because we have been dealing knowing or unknowingly with cyber security. But it's easier to define the issues arising with cyber security. That being said I think it is very important to be specific about the type of cyber security issues that we deal with and which sector are we referring to e.g. private, public, banking etc.

The more we specific we are the more easier it will be for the general public to understand the issues of cyber security, especially when people still haven't really grasped the dangers of the cyber world and where cyber security has stepped in and more importantly the funding needed to establish a fully functional cyber security mechanism in tackling threats from international level to national to inter business level.

The brutal truth is has been meeting on top of meetings around the world with establishment of organisations and bodies but I have not yet seen any concrete international cyber security policy out there where by it can be a benchmark for all nations that are serious about cyber security.

Do you think this might be because of lack of understanding about cyber security and how generalised the term is?

From Andrew Cormack:

"Personally I've found that it has so many different interpretations (both across and within sectors) that it's almost meaning-free. So any discussion that mentions it ends up either as a discussion of what the participants mean by it, or at worst as a very long and complete miscommunication between people each talking about their own interpretation. But today's call also made me wonder whether it's actually a barrier to learning from past experience - anything that pre-dates the invention of the term can't be relevant to it. So maybe trying to explain that "cybersecurity" consists of a number of pre-existing fields (information security, on-line crime, incident response, etc.) can make it easier to learn from those previous fields? As I said in the call, I've recently discovered that I've been doing "cyber security" for twenty years.

And on a related issue we've recently had a nice (for illustration purposes)/horrid (for network defence purposes) illustration of the importance of the label under which you work. Our UK national CSIRT recently moved to be part of the National Cyber-Security Centre: "a part of GCHQ", according to its logo. That connection was sufficient that an announcement of a possible RPZ feed of malware sites was pretty much universally reported, including by journals that should understand the difference, as "UK announces national firewall". See, for example, the Financial Times: https://www.ft.com/content/85549652-79d1-11e6-97ae-647294649b28"

Messages from the 2016 European Dialogue on Internet Governance (EuroDIG) and the 2016 Asia-Pacific Regional IGF (APrIGF)

During a workshop[11] (*Workshop 5: Cybersecurity revisited, or are best practices really best?*) held at the **2016 European Dialogue on Internet Governance (EuroDIG) held from 9-10 June 2016**, the following messages from participants emerged from the meeting which further indicate the demand from the community for further dialogue on cooperation and collaboration in cybersecurity work:

- *People tend to cluster together and collaborate within trusted communities, because with a trusted relationship something can be done. How to broaden this cooperation by binding with other clusters/communities?*
- *We need to collaborate to get things done, and the essential point is then to create trust between stakeholder groups: successful examples were when battling spam and cooperation between CERTS and LEA's. It can be done.*
- *Diplomatic communities (with a so called 'military tradition') and technical communities often mean something completely different when talking about security. There is a massive gap. But they are talking to each other and there certainly is an intention to continue the dialogue.*
- *How to keep the different 'clusters' open, where issues are discussed? More transparency is necessary when it comes to public-private-partnerships: all stakeholders should (be able to) participate.*
- *There is a multitude of platforms and initiatives working on cybersecurity, all spending money and doing capacity building: but are they indeed open and transparent, and what effect do they have and how to bring them together? This is an open question…*[12]

The Synthesis Document[13] from the **Asia-Pacific Regional IGF held from 27-29 July 2016** also stated:

"II. Security

Cybersecurity, the protection of information systems from damage and disruption, is critical not just to the stability of cyberspace, but also increasingly important to the physical world. Whether it is security, stability & resiliency of the Internet infrastructure or security of network and information systems, collaboration is needed to mitigate and prevent cyber security incidents within and beyond the Asia Pacific region, and the setting of global encryption standards is encouraged.

Draft Outcome Document from the African Internet Governance Forum (AfIGF) 16-18 October 2016:
http://afigf.org/sites/default/files/2016/docs/REPORT%20AFIGF%202016%20Draft%20outcome%2018102016_evening_rev1.pdf

Conclusions and Recommendations from the Plenary Sessions:

Session 5: Security and Privacy issues in the Internet:

---

[11] http://eurodigwiki.org/wiki/WS_5:_Cybersecurity_revisited,_or_are_best_practices_really_best%3F#Messages

[12] Messages from 2016 EuroDIG Workshop 5:
http://eurodigwiki.org/wiki/WS_5:_Cybersecurity_revisited,_or_are_best_practices_really_best%3F#Messages

[13] 2016 Asia-Pacific Regional IGF Synthesis Document: http://comment.rigf.asia

"African member states should sign and ratify the AU Convention on Cybersecurity and Personal Data Protection. In this context, they should implement relevant regulations related to Access to Information, data protection, privacy and cybercrime.

"Reinforce capacity building on Internet governance issues as education and cybersecurity."

Part II: Synthesis of contributions received[14] in response to the call for contributions[15]

Following a series of virtual meetings[16] and consultations via the BPF Cybersecurity mailing list[17], on 11 July 2016 the IGF Secretariat launched a public call for contributions on the IGF website inviting the IGF community to submit responses to the following questions:

- *What are the typical roles and responsibilities of your/each of the stakeholder groups in making the Internet a secure and safe place for people to socialize and conduct business?*
- *What are some of the typical communication mechanisms between stakeholder groups to discuss cyber security related concerns?*
- *How can cybersecurity cooperation and collaboration be enhanced particularly in developing and least developed countries?*
- *What are some common problem areas that stakeholders encounter when trying to enhance cooperation and collaboration?*
- *What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?*
- *What are some examples of best practices in 'Cyber security Situational Awareness' where different organizations have worked together, specifically with law enforcement agencies and other specialists?*
- *What are other related or different topics that your organization would like this BPF to address moving forward, both in 2016 and beyond?*

The following section compiles and synthesizes the contributions received by the community to these questions. Some contributions are summarized while others are included verbatim. All contributions can be accessed and reviewed in their entirety on the IGF website here and in Annex I of this document.

---

[14] http://www.intgovforum.org/cms/191-igf-2016/bpf-2016/3111-list-of-contributions-2016-igf-best-practice-forum-bpf-on-cybersecurity

[15] http://www.intgovforum.org/cms/best-practice-forums/bpf-cybersecurity

[16] http://www.intgovforum.org/multilingual/content/bpf-cybersecurity

[17] http://www.intgovforum.org/mailman/listinfo/bp_cybersec_2016_intgovforum.org

- ***What are the typical roles and responsibilities of your/each of the stakeholder groups in making the Internet a secure and safe place for people to socialize and conduct business?***

Contribution from the Freedom Online Coalition (FOC):

The roles and responsibilities of stakeholders are evolving in making the Internet a secure and safe place for people to socialize and conduct business. It is clear that security is no longer just the purview of governments and that it is increasingly a multistakeholder imperative. With cybersecurity and cybercrime challenges increasing in frequency and complexity there is a need for all stakeholders to work together to address these in a manner that preserves human rights, particularly privacy and free expression.

The call for cybersecurity policies to be developed in a more open and inclusive manner with greater protections for human rights has been growing:

- The Seoul Framework[18] that resulted from the Seoul meeting of the London Process in 2013 states that it is "necessary to continue to work together towards ensuring a trusted, secure and sustainable environment in partnership with multiple stakeholders, including international organizations and the private sector."
- The 2014 NETMundial Multistakeholder Statement[19] noted, inter alia, that "initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, private sector, civil society, academia and technical community."
- And, the Chair's statement[20] at the 2015 GCCS meeting in The Hague urged governments "to ensure that cyber policy at national, regional and international level is developed through multistakeholder approaches, including civil society, the technical community, businesses and governments across the globe."

Despite the recognition that cyber issues should be dealt with involving all stakeholders, there are few fora in which cybersecurity related concerns can be discussed on a multistakeholder basis. Various issue specific meetings may be held on cybersecurity matters to which other stakeholders are involved, but the degree to which civil society are engaged and welcomed is minimal, particularly in cybersecurity policy and norm- setting processes. Much work remains to be done to realize and put into practice the increasing calls for multistakeholder approaches – now is the time for all stakeholders to work together to make this a reality.

The Freedom Online Coalition Working Group 1 on "An Internet Free and Secure" has undertaken the following mapping of cyber security spaces and processes which assesses the degree to which they are open or not to stakeholders:

https://www.freedomonlinecoalition.com/wp-content/uploads/2015/05/Mapping-Brochure-WEB-1.pdf

This mapping exercise clearly illustrated the degree to which cybersecurity processes and fora remain closed to stakeholders and particularly civil society.

Contribution from Mr. Fotjon Kosta, Albania:

---

[18] http://www.mofat.go.kr/english/visa/images/res/SeoulFramework.pdf

[19] http://netmundial.br/netmundial-multistakeholder-statement/

[20] https://www.gccs2015.com/documents/chairs-statement-gccs2015

The contribution from Mr. Fojon Kosta highlighted the 2013 'Behavioural Code' in Albania as an important agreement aimed at making the Internet a more secure and safe place. In this agreement all mobile companies, ISPs (Internet Service Providers) and the Ministry of Technology and Information officially committed to protect children from Internet risks. This code provided new services to raise Internet users' security.

Contribution from Mr. Segun Olugbile, Nigeria:

i. The Nigerian ICT & Cybersecurity stakeholders' forum provides local awareness for policy makers on cybersecurity and public Internet safety. The forum collaborates with heads of government agencies relevant to ICT development, telecommunication regulation and captains of industry in the ICT industry to build trust and entrench Internet user confidence on the use Internet as a tool and a platform.

ii. We engage the public on cybersecurity awareness through consistent participation in the Nigeria Internet Governance and similar event such e-Nigeria Summit where we ensure regular discussion on a secure cyberspace, share emerging issues on Internet safety as well as provide relevant capacity building on Personal & Corporate Internet Safety Responsibility (PCISR).

iii. We engage the use of social media apps most especially WhatsApp to create discussion forum where instant Internet security incidents and mitigation reports are distributed and shared among individual members of the forum on real live and upwardly mobile basis. This approach has helped deescalate spread of the incidences and provide community awareness.

iv. We engage in local high level political discussions with senior public officers and political offices holders within the executive and legislative arms of the government on possible policy and legislative intervention on cybersecurity.

v. The group collaborate with key industry players and industry regulator on the development of technical code of conduct for the ISP and operators in the Internet Industry.

Contribution from the Association for Progressive Communications (APC):

Cybersecurity initiatives should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and user's[21].The respective roles and responsibilities of stakeholders should not be set in stone, or defined definitively at one point in time. Rather they should be interpreted in a flexible manner with reference to the issue under discussion. From the 2014 NETmundial Multistakeholder Statement, "initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, private sector, civil society, academia and technical community."[22]Furthermore, policy processes should actively seek out experts from all stakeholder groups that together comprise a wide range of contexts and experiences.

States are the duty bearers for human rights and security (including the right to personal security) in the international system. They have a positive obligation to provide a minimum standard of protection for the lives, integrity and personal security of individuals in their jurisdiction or under their effective control. States have obligations and duties under international law to respect, to protect and to fulfil human rights. The obligation to respect means that states must refrain from interfering with or curtailing the enjoyment of human rights. The obligation to protect requires

[21] netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
[22] netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

states to protect individuals and groups against human rights abuses. The obligation to fulfil means that states must take positive action to facilitate the enjoyment of basic human rights.

These obligations extend to the digital environment, as the same rights people have offline must also be protected online.[23] Governments have committed to "address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development."[24]

The private sector must engage in multistakeholder policy spaces alongside civil society and governments and uphold their responsibility to respect human rights. As the UN Guiding Principles on Business and Human Rights[25] lay out, corporations have the responsibility to respect human rights, including by acting with due diligence to avoid infringing on human rights and addressing adverse impacts with which they are involved, and to provide victims access to effective remedy.[26] Not only should we expect the private sector to follow international law, but non-binding standards and protocol norms as well. Products of the private sector should respect human rights by design. Likewise, where the private sector conducts research and development, its standards and protocols should be rights-respecting by design; for example, user privacy should be considered as inherently valuable as efficiency.

There is a recognition that the technical community cannot work alone, which is why we have seen recent reports such as from David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, supporting the implementation of encryption and anonymising tools as critical for human rights[27]. Kaye recommended that States, international organizations, corporations and civil society groups should systematically promote access to encryption and anonymity without discrimination and engage in a campaign to bring encryption by design and default to users around the world.

Contribution from the Organization of American States (OAS) Cybersecurity Program:

The Organization of American States (OAS) Cybersecurity Program's efforts are geared toward three specific objectives:

a. Increasing access to knowledge and information on cyber threats and risks;

b. Enhancing the technical and policy capacity of governments and critical infrastructure operators to detect cyber threats, respond to cyber incidents, and combat both;

---

[23] See Human Rights Council Resolution 20/8 (2011) on "The promotion, protection and enjoyment of human rights on the Internet". ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

[24] See Human Rights Council Resolutions 26/13 (2014) and 32/13 (2016) on "The promotion, protection and enjoyment of human rights on the Internet". ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/13 and ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/32/L.20/

[25] UN Guiding Principles on Business and Human Rights. (2011). www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[26] Sullivan, D. (2016). *Business and digital rights: Taking stock of the UN Guiding Principles for Business and Human Rights in the ICT sector*. APC. https://www.apc.org/en/system/files/APC_Business_and_digital_rights.pdf

[27] Kaye, D. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://www.justsecurity.org/wp-content/uploads/2015/06/Kaye-HRC-Report-Encryption-Anonymity.pdf

c. Promoting more robust, effective and timely information-sharing, cooperation and coordination among cybersecurity stakeholders at the national, regional and international level.

The Program's stakeholders include government entities, the private sector, academia, civil society and the general public from the OAS member states. Each stakeholder grouping participates in the cybersecurity supply chain at different stages, either as a supplier or an end-user as each has a role to play in keeping their activities secure. As it relates to our activities, each stakeholder grouping has made every effort to participate and contribute to workshops, reports and the develop process for national cybersecurity frameworks. Our workshops include different topics, ranging from critical infrastructure protection to cybersecurity and freedom of speech in the web, and the participation of experts and attendees with different backgrounds. Our reports are prepared based on a comprehensive understanding of cybersecurity with the contributions of stakeholders from different sectors. Our last report, "Cybersecurity: Are we ready in Latin America and the Caribbean?[28]" jointly prepared with the Inter-American Development Bank, is a good example of this collaborative work. Finally, the development of national cybersecurity strategies involves the participation of representatives from different stakeholders since its inception in order to build a common national view on cybersecurity.

Contribution from the National Cyber Security Centre - Finland (NCSC-FI):

- First of all, we have roughly a dozen sectoral cooperative networks (energy, finance, vendors… + a few networks for different authorities). These networks cooperate on two levels. The first level is the daily information sharing via email lists, IRC and portals. The second, and more closed cooperative level, is the face-to-face meetings among selected peer organizations.
- The face-to-face meetings bring technical personnel together in order to share information, best practices etc. on the level the cooperative group wants it to take place in. There are no "responsibilities" as such except active participation and information sharing on threats, current challenges, success stories etc.

Contribution from Global Partners Digital (GPD):

Evolving understandings of cybersecurity make efforts to ensure the Internet is a secure and safe place an important focus of policy that requires input from multiple stakeholders. Starting from a dominant technical perspective of cybersecurity and focusing on protecting information infrastructure, debates around cybersecurity have rapidly broadened, bringing in many issues from cybercrime to secure access policies to data ethics and human rights under its banner.

From its inception, the protection of the Internet was taken on mainly by governmental actors and the technical community. As the Internet has grown and become more a part of our economies and societies, more capacity - and indeed responsibility - for keeping the Internet secure has passed into the hands of private sector actors. This is because in many cases critical infrastructure is owned by businesses and public-private sector partnerships are considered essential to ensuring robust cybersecurity.

This has resulted in a situation whereby much of the policy and technical measures discussed in cybersecurity debates are defined primarily by private and state actors. While their involvement is vital, the dominance of these state and commercial perspectives has often put an emphasis on the protection of systems rather than the individual, and has led to cybersecurity policy approaches that often appear to pit security against human rights which can lead to curbs on fundamental

[28] https://publications.iadb.org/handle/11319/7449

rights. This might mean more restrictions on content and freedom of expression, more disproportionate measures like mass surveillance, and more measures to undermine anonymity in the interests of furthering security interests.

Much work by civil society and other non-state actors has shown that this is a false dichotomy. Cybersecurity and human rights in fact depend on each other. Security is not something enacted on something to mitigate risk and harm - security is a positive concept, importantly associated with a *person's* freedom and capacity to act; without security the individual cannot fully exercise their rights. This rights-based perspective that above all focuses on people as the referent object of cybersecurity - rather than systems - is often missing from debates on cybersecurity policy.

With increasing challenges with regard to ensuring a safe and secure Internet, it is therefore vital for all stakeholders to work together to address these in a manner that preserves human rights. This imperative has already been recognised in the call for multistakeholder participation in many cybersecurity-related processes from the London process to NetMundial. But more work remains to be done to ensure the main policy making spaces are opened up to meaningfully incorporate multistakeholder input. Engagement with civil society is still minimal, and strikingly absent from most cybersecurity policy and norm-making processes.

- ***What are some of the typical communication mechanisms between stakeholder groups to discuss cyber security related concerns?***

Contribution from the Forum of Incident Response and Security Teams (FIRST):

The communications mechanisms used by CSIRT to interact with their constituency and peers are diverse. Most CSIRT communications involve notifying others of problems or vulnerabilities: asking others to disclose information about perpetrators is a role for law enforcement agencies. Law enforcement reduces the number of criminals: CSIRTs reduce the opportunities for committing crimes. Below we are referencing a small set of messages that are in use by the CSIRT community:

- Standardized protocols, such as the Network Abuse Reporting framework X-ARF are used by the community to report abuse originating from a particular network. Participants in the incident response community can develop X-ARF messages to flag a particular host as emanating malicious traffic, and send these reports for automated or semi-automated processing by the network owner;

- Within the CSIRT community, several tools are in use to collect, assess and re-distribute information to the correct stakeholders. Examples include Abuse Helper, which allows automated processing of incident notifications, and the Malware Information Sharing Platform (MISP) which allows automated exchange of incident indicators.

- E-mail is still a common method for reporting security incidents. A CSIRT may both receive messages from other network owners or data sources on events that originate or occur within its constituency (e.g. compromised web sites, phishing, or a malicious host scanning another network), or may send them (e.g. notifications of a phishing site that affected a constituent).

Confidentiality of information is typically important, especially when working with a stakeholder that is in the process of mitigating a security incident. Early knowledge of such an incident by either the adversary, or others could make an effective response more difficult. Within the community, standardized protocols such as Transport Layer Security (TLS) are most often used for automated tooling, and Pretty Good Privacy (PGP) is the de facto standard for e-mail communication.

As a community, automating information exchange where possible, and ensuring CSIRT's ability to process information at an increasing pace is extremely important. CSIRT can often be resource

constrained in terms of qualified analysts, and allowing them to focus on harder problems that require expert review is critical.

However, it is important to clarify that prior to any automated exchange taking place, it is crucial for stakeholders to set expectations around how the data will be used. Sharing indicators may not be helpful if they are not used correctly, or are used for different purposes than intended. While there are typically many technical means of addressing a security incident, it is most important that goals are aligned and expectations are clearly set.

Several members of the wider incident response community have built specific partnerships and programs to enable them to work effectively with other parties on similar problems. Examples of these are well described in Proactive detection of Network Security Incidents, published by the European Network and Information Security Agency.

Mr. Fotjon Kosta, Albania:

The contribution noted that the Albanian Government has made multiple agreements and has implemented several mechanisms between stakeholders groups related cybersecurity including the establishment of the Albanian CIRT in 2011

Mr. Segun Olugbile, Nigeria:

The Nigeria ''Stakeholders Roundtable on Cybersecurity'' was created to foster communication on policy issues, cooperation, and understanding of common emerging Internet security incidences among local stakeholders.

NCSC-FI:

- As stated, we are using closed email lists, IRC, portals and face-to-face meetings. Arguably the most valuable tool is, however, the face-to-face meetings.

APC:

In 2015, the Freedom Online Coalition working group "An Internet Free and Secure" (FOC WG1) published a mapping of cybersecurity policy-making spaces. What they found was that nearly 40% of those fora were closed to or placed limits on civil society participation. The main problem of communication between stakeholder groups is that states close their processes for reasons ranging from domestic security to status quo policy making. The private sector's cybersecurity practices are protected intellectual property. At best, fora like the Global Conference on Cyberspace invite civil society participation that is neutralised by a full schedule of presentations and panels, while bilateral meetings between states and the private sector are scheduled in parallel. Another example is committees or working groups that are multistakeholder but that only produce very high-level recommendations or agreements that are non-binding and demand no accountability from even the stakeholders who produced them.

OAS:

a. The OAS Cybersecurity Program has a twitter account which facilitates the easy transmittance of information and communication among the followers.

b. The OAS Cybersecurity Program has a mailing list in which anyone can participate. This mailing list announces the Program's next activities and recently published reports.

c. The Program has also been developing a virtual hemispheric network of CSIRTs which seeks to facilitate real-time communication and information-sharing between CSIRTs in the Americas.

d. In the development of National Cybersecurity Frameworks, the program facilitates multi-stakeholder roundtables and national workshops to discuss cybersecurity issues facing member states.

e. The publication of cybersecurity reports that benefits from the input of all member states in providing accurate and current data on their national cybersecurity reality.

f. The hosting of sub regional, regional and international cybersecurity crisis management exercises in collaboration with private sector and national and international government entities.

- ***How can cybersecurity cooperation and collaboration be enhanced particularly in developing and least developed countries?***

APC:

The role of the technical community includes, in some national and regional contexts, the establishment of Computer Emergency/Incident Response Teams (CE/IRTs) and Public Key Infrastructure in order to support resilient implementations of secure protocols and standards. At a minimum, we would like to see more emphasis placed on research of these types of institutions so as to strengthen them and model human rights-respecting best practice.

There is a need for more civil society involvement in cybersecurity debates in all countries, and in particular in developing countries. Furthermore and in parallel with increased participation, more opportunities for education and awareness raising among civil society groups on issues of cybersecurity should be supported.

OAS:

a. Engagement of political leadership is critical as this will ensure the continuation of cybersecurity initiatives and incorporation of cybersecurity concerns into cross cutting policy issues, such as economic development and national infrastructure expansion projects.

b. Staging of Regional meetings geared towards networking and building networks on various levels (private sector, academia and government counterparts).

c. Engagement with stakeholders from different sectors since the beginning of the formulation of cybersecurity policies through participatory and deliberative procedures (e.g., roundtables, online tools) in order to build trust and confidence and ensure the transparency and accountability of the entire process.

GPD:

The Global Partners Digital video series "How to Engage in Cyber Policy"[29] is one initiative to help bridge the gap - both in knowledge and also in terms of understanding different perspectives on cyber policy issues. The series is aimed at any actor who holds an interest in developing rights-based policy, regardless of stakeholder group, and aims to give a holistic understanding of cyber issues that see security issues and human rights as mutually reinforcing, resulting in more effective and empowering policy measures, globally.

For cybersecurity cooperation and collaboration to be enhanced globally - and particularly in global south countries - the first step is to create a level playing field in terms of knowledge, skills and capacity for engagement. This has been acknowledged through multiple capacity-building projects focusing largely on Internet policy and governance, but less so in the more specialized space of

[29] https://www.youtube.com/channel/UCow9ZGJMNsZtAkz4ZvTtcJA

cyber security and human rights. It's important to appreciate that cybersecurity and human rights capacity-building will require sustained engagement over time, building the skills, knowledge and overall capacity of human rights defenders and others to engage in an informed manner in dialogues, exchange of information and finally the development of solutions for cybersecurity challenges that are rights respecting by design. We believe that this video series makes an important contribution to this growing capacity building effort.

NCSC-FI:

- It is very important to define the scope of the cooperation. We have tried to keep the cooperation as close to "real world" technical problems as possible. There has to be a clear and understandable value proposition. As a government authority we try for example to provide participants information they would not otherwise have.
- Let the development of cooperation take time. It is important that different players first get to know each other. Before that no true cooperation can take place. This concerns especially the face-to-face meetings.
- The cooperative bodies should have as much homogeneity as possible. This helps focusing the subjects.
- Make sure everyone knows who are involved and why they are involved.
- Make sure everyone knows what the cooperation is for; a "code of conduct" (who, why, how, when) should be drafted together with the participants. This also helps the participants to justify the participation within their own organizations.
- Make sure that the people who participate in the cooperation are empowered enough and informed within their organizations.
- Also, try to identify at least a few active persons representing the industry beforehand. Contact them and ask them to take active role especially in the beginning in order to break the ice and get things going.
- When putting face-to-face meetings in place, try to find someone from the industry to act as the chair for the group.
- Make sure you have Traffic Light Protocol or other formal rules concerning the level of confidentiality and dissemination of information in place.
- Keep the number of participants as small as possible. This helps building the trust among participants.
- If you are a public sector organization, take active role in the beginning. Usually in the beginning it is more useful to start with a top down approach. It is possible to move later into a model where the industry members take more active role.
- Conduct a "customer satisfaction" survey regularly, preferably once a year.

- ***What are some common problem areas that stakeholders encounter when trying to enhance cooperation and collaboration?***

From Fotjon Kosta, Govt. of Albania:

The most common problems areas are: lack of legal framework, lack of financial resources and human resources, social and political issues and lack of capacity building.

APC:

Overwhelmingly, fora's for cooperation and collaboration on cybersecurity issues are closed to civil society. Civil society is often unable to find the venues to engage, while states and the private sector do not look to spaces like the IGF, where there is robust civil society participation, to address cybersecurity concerns. When opportunities are opened, the general lack of transparency and familiarity with processes and actors makes it difficult to engage meaningfully. Spaces where civil society is invited to participate prepare no binding or accountability mechanisms.

The dominant narratives around cybersecurity are a significant barrier. Governments from across the political spectrum insist on pitting security and human rights against one another, when in fact the trade-off of some "security measures" (like building in backdoors) is actually security versus security. Many governments assert that security is good enough even if the right to privacy and the security of individuals are not fulfilled, and thus sacrifice human rights for the sake of this top-down notion of "security". The ubiquity of the framing that security and privacy are incompatible means that civil society engagement is focused on upsetting this ideology rather than bringing concrete policy recommendations for rights-respecting cybersecurity.

FIRST:

For CSIRTs to effectively work with each other, or other peers within the community, trust is a crucial requirement. Trust is typically not established through legal agreements, but through a history of working with each other. This work contributes to building trust in at least two ways:

- It ensures both organizations have an accurate understanding of the actions the other organization will take. For instance, when indicators of a security incident are provided, a CSIRT can trust the information will be used to remediate the source of the incident, rather than purely for investigative or intelligence purposes, which may not assist the CSIRT in mitigating the incident.

- It ensures organizations have an understanding of the effectiveness and capability of the other CSIRT. If multiple reports have not led to successful remediation, or led to action which was counterproductive (for instance simply taking down malicious content, which continues to reappear, rather than addressing the issue comprehensively), a CSIRT may be less inclined to share information in the future. At the very least, it will need to check that both parties have a common understanding of the incident response services being offered and provided.

Maturity and trust help avoid these misunderstandings. Problems can often arise when there is no CSIRT present, but the incident response role is performed on an ad-hoc basis. For instance, in the product security world, organizations may react defensively, or even threaten legal action, when a security vulnerability is reported, rather than implementing and executing on known vulnerability coordination steps, such as defined by ISO 29147:2014. Building incident response maturity helps address and prevent these issues.

In our experience, developing trust is easiest when the objectives of both organizations align. When both organizations have as goal to remediate the incident and restore operations, they both see value in the information exchange. Trust does not develop when one or both organizations are perceived as having a different goal, an issue which sometimes appears when a CSIRT is established within a law enforcement or intelligence agency.

NCSC-FI:

- Not knowing the right level of abstraction and technical details in which to have the discussions

- Among very competitive areas, the participants may be hesitant to provide information. Legislation may even prohibit sharing of some security information between companies if it distorts competition.

● ***What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?***

Contribution from the Information Technology - Information Sharing and Analysis Center (IT-ISAC):

The concept of ISACs was introduced in the United States in Presidential Decision Directive-63 (PDD-63), signed May 22, 1998. While initially focused on the United States, the ISAC concept has spread globally, and many U.S. based ISACs now accept membership from companies outside the United States and operate globally. 21 ISACs coordinate and collaborate through the National Council of ISACs (www.isaccouncil.org).

ISACs are trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation among security teams. Typically non-profit organizations, ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

ISACs have demonstrated success in providing operational services – such as risk mitigation, incident response, and information sharing – that help security and response teams protect critical infrastructures.

Preparedness & Operational Considerations

1. Incident Response. A key service of an ISAC is to provide critical infrastructure sectors with actionable intelligence leaders need to make informed decisions that enable incident response teams to more quickly identify and respond to incidents. Whether through information sharing portals, collaborative lists, or other arrangements, ISACs can harness industry specific analysis to contextualize member-provided, open-source, for-cost services and public-sector-provided threat news. ISACs can help incident response teams develop a sound understanding of the threat environment and the communities' relevant risks, providing a trusted community that enables teams to discuss how to manage their organizational risks and concerns.

2. Training. ISACs can provide your security teams with access to training and discussions with peers that cover contemporary, pressing topics to the industry at large. This sort of community exchange, using resources from across a wide spectrum of disciplines and making it applicable and collaborative for a specific community, is only possible through an ISAC or similar organization capable of taking a sector-wide / community-wide view of the threat environment, being able to understand and process the relevant risks, and helping community members identify their greatest concerns.

3. Exercise. Many ISACs have participated in a variety of exercises with their members and with partners. From high-level exercise events validating the information sharing and collaborative processes between ISACs and partners to sector-specific drills exercising intra-ISAC processes and procedures to ensure readiness to respond to major threats and events, ISACs help members develop and test their ability to react to the dynamic threat environment. Some ISACs can also provide resources or contacts to help members conduct their own exercises ensuring robust preparedness across sectors.

4. Operations. Many incident response teams formally integrate ISAC membership into their Concept of Operations and other operating policies. These help to operationalize and institutionalize the relationship between the ISAC teams the member incident response teams. Setting policies on integrating with ISACs also enables incident response teams to understand and share information that is relevant to other ISAC members.

Information Sharing and Analysis Center's (ISACs) help incident responders from critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyse and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

Contribution from the Computer Incident Response Center Luxembourg (CIRCL)

CIRCL (Computer Incident Response Center Luxembourg) is a government-driven initiative designed to gather, review and respond to computer security threats and incidents. It's the CERT for the private sector, communes and non-governmental entities in Luxembourg.

CIRCL is operated by SECURITYMADEIN.LU, which has even broader missions in the area of cybersecurity, from awareness raising, both via national campaigns as well as by dedicated sessions with specific target audiences (children, youth, elderly people, etc.) (e.g. https://silversurfer.lu/); via organisational security through the federation of risk management methodologies and other information security governance tools (e.g. MONARC - https://www.cases.lu/index-quick.php?dims_op=doc_file_download&docfile_md5id=56ee6ff569a40a5b52bed0e526a6a77f); up to fostering the cybersecurity ecosystem in Luxembourg, mainly by promoting information sharing, collaboration and co-operation among stakeholders (e.g. https://securitymadein.lu/cybersecurity-breakfast/).

The setup of SECURITYMADEIN.LU, 6 years ago, with its threefold mission, covering behavioural, organisational and technical aspects of cybersecurity, has become the de facto centre of excellence in this area for Luxembourg. Communication-wise, the different stakeholders are addressed in a regular fashion, via press and media coverage (e.g. http://www.itnation.lu/62000-cyberattaques-au-luxembourg/), awareness campaigns (e.g. https://www.bee-secure.lu/fr/outils/campagnes/clever-cloud-user), conferences (e.g. https://2016.hack.lu/) and training (e.g. https://circl.lu/services/misp-training-materials/).

Over 4 years of experience in malware and threat sharing, via MISP (https://circl.lu/services/misp-malware-information-sharing-platform/) shows that co-operation and collaboration is key in cybersecurity, not only to avoid duplicate work and analysis, but also in respect to less mature entities, being able to profit from the experience and expertise of others and as such develop faster thereafter. MISP brings together specialists from different areas, like malware reversers, security analysts, intelligence analysts, law enforcement, risk managers and banking fraud analysts. Legal restrictions, like law enforcement frameworks, but also practical issues, high risk of information leakage, a "nothing- to-share" mentality or alike are difficulties that we encountered.

Nonetheless SECURITYMADEIN.LU continues its investment, development and promotion of MISP as well as MONARC; because we believe in the "sharing is caring" principle and especially focus on bringing together specialists with different competences and knowledge.

A nice example is the "committee C", as we call it, which is a regular meeting of the local CERT community, law enforcement, attorneys and judges as well as intelligence people to exchange on relevant information and co-operate on common cases.

At the level of organisational Cybersecurity, risk management has become the main driver, not only because the European legislator has seen its usefulness and integrated aspects of risk-based approaches in recent directives (e.g. NIS directive) and regulations (e.g. GDPR), but also businesses need to get better knowledge and grasp on their risks. MONARC builds on this and especially focuses on providing a solution to empower SMEs with efficient tools and access to the expertise needed, by reducing the time for a risk analysis by up to 80%. These figures were achieved in the area of local government and municipalities in Luxembourg, due to extreme overlapping needs and procedures. Currently other sectors are being addressed with this same mutualisation scheme to achieve similar efficiency.

Tools, platforms and other technological "helpers" are often modelling how people and organisations work together. Especially in cybersecurity, tools are critical to conduct incident response, make information sharing easy and enhance proactive notification. All these tasks involve huge volumes of data and can only be efficient with performing and adequate tools. When designed and operated by the "user community" itself, tools tend to better support the work of the community and especially security-wise do a proper job.

Our two main platforms, MISP and MONARC, needed improvements in many different areas and by reducing the development cycle, the communities could benefit from their feedback in a timely fashion. Tools, if heavily used and appreciated by the communities, can even influence the legal framework or highlight current limitations of a specific regulation.

Something else that we have seen in our past experiences is the importance in the distribution of the tools. Only those that are widely available and not restricted by complex confidentiality agreements, have succeeded and got high acceptance of their user communities.

Beyond these considerations, guidelines to build a "culture of security" for economic and social prosperity are depicted nicely in the 2002 and 2015 OECD documents on security (please find them attached for your convenience). They are both still valid and give great insight for large-scale or national cybersecurity strategies.

Contribution from Together Against Cybercrime (TaC)[30]:

TaC – Together against Cybercrime International is a non-profit making civil society anti-cybercrime organisation established in France and working at local, national, European and international levels. TaC International works in the field of cybercrime/cybersecurity and child online protection and advises different entities on cybersecurity strategies. TaC is also actively involved in Internet governance issues by stimulating discussion on the use of information and communication technologies (ICTs) by vulnerable people and initiating debate in the format of youth and teenager dialogue.

GPD:

Cybersecurity policies, laws, and strategies can have serious implications for human rights, and the need for a strong human rights voice in cyber policy making processes and debates has thus become crucial. However, all too often, the spaces they are made in can seem closed and inaccessible to many actors, especially civil society. This results in important decisions on cyber policy being taken by a narrow range of security actors, behind closed doors and without the crucial scrutiny, insight and expertise that human rights defenders can provide.

[30] https://againstcybercrime.org/

Earlier this year, Global Partners Digital launched a new global cyber capacity building programme, which aims to help human rights defenders develop the tools, skills and knowledge they need to engage effectively in cyber policy debates.

One core element of the programme is the online series 'How to engage in cyber policy: tools for human rights defenders'.

A key focus of this series has been on the relationship between cybersecurity and human rights. "Cybersecurity" has become a catchphrase in a whole range of discussions dealing with different aspects of cyber policies, often pitting security against human rights. Gaining the basic knowledge and resources needed to engage in these debates can be challenging.

The series aims to provide a starting point for human rights defenders all over the world to kick-start debates on cyber policies that support and promote human rights and security in a balanced manner.

The video series was developed in collaboration with an Advisory Board, and in consultation with cyber policy experts worldwide, who helped identify pressing issues in the target regions and shape the curriculum.

The series is structured around five modules: the first four each focus on a different aspect of cyber policy - human rights, cybersecurity, regulatory frameworks and cyber capacity building - with a final regional module highlighting how these apply in Africa, Asia and Latin America.

Each video was developed collaboratively with cyber policy experts from around the world, and takes participants through a key cyber issue or concept — explaining how it relates to human rights, who the key actors are, and how and where to engage. Each module is also accompanied by a live Q&A session, giving participants the chance to discuss the issues with field experts from around the world. (Watch the recording of the Q&A sessions for the modules on Human rights and Cybersecurity.)

The videos were designed as a *long term, sustainable and lasting resource* to be used in the future. Although the videos feature case studies that might become outdated, the concepts outlined form the core of crucial debates on cybersecurity policy - particularly the importance of multistakeholder engagement in defining cybersecurity and the threats perceived under its banner, and the importance of human rights as a crucial underpinning of all debates surrounding cyber policy. They can be watched individually or as a whole, giving people flexibility to choose what topics they would like to focus on and in which order.

The series was designed as a *public resource, open to everyone interested*. All videos are licensed under Creative Commons so people are free to share them. They have already been used as a resource in other training programmes, like the Middle East and Adjoining Countries School of Internet Governance (see https://twitter.com/SMEX/status/763655273911312384 ; https://twitter.com/SMEX/status/763652370224058368)

The videos have English subtitles, which make them easier to understand for non-native speakers, and are currently being translated into more languages to reach broader communities. This is being done on a voluntary basis by organisations and individuals who wish to use the videos as a learning resource - illustrating how much demand there is for videos like these to fill gaps in knowledge among civil society actors.

OAS:

Exchange of best practices and ideas during regional workshops. These regional workshops provide a unique opportunity for stakeholders from Latin America and the Caribbean to discuss their

problems, to share lessons and cybersecurity capacity, as well as to build a common understanding of cybersecurity.

FOC:

The Freedom Online Coalition Working Group 1 - "An Internet Free and Secure" (FOC WG1) is a notable and highly functioning example of multistakeholder collaboration on cybersecurity. The purpose of FOC WG1 has been to bring a human rights framing to ongoing cybersecurity debates. It aims to develop, through multistakeholder dialogue, meaningful outputs that feed into existing cybersecurity processes and the creation of new, more effective, human rights enhancing cybersecurity policy.

The Working Group's purpose, composition and blog series can be found here:

https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-%20group-1/

The WG was created as a multistakeholder exercise by design, noting UNGA Resolution 57/239 on the creation of a global culture of cybersecurity and in particular the Annex on Elements for creating a global culture of cybersecurity notes the importance of stakeholders working together. FOC-WG 1 can serve as a model for successful multistakeholder collaboration on cybersecurity between the private sector, civil society and governments. The work involved Internet policy, cybersecurity and governance experts from across stakeholder groupings, was driven by collaborative and open dialogue and resulted in multiple significant outputs. Notably, the WG has developed the following definition of cybersecurity focussed on information and individual security:

https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-%20group-1/blog8/

In order to advance the normative debate on cybersecurity, the WG developed a set of recommendations that promote greater stakeholder-driven and human rights respecting approaches to cybersecurity. These recommendations were developed with the aim to provide guidance to all stakeholders involved in cybersecurity matters, and in particular those involved in developing and implementing cybersecurity policies and frameworks. They are designed to encourage stakeholders to incorporate the protection and promotion of human rights in all matters related to cybersecurity and to ensure that cybersecurity policy is rights-respecting by design.

And, as a step towards facilitating greater stakeholder engagement in cybersecurity debates, the working group conducted a mapping exercise to identify main global spaces where cybersecurity is being discussed. The main objective of this exercise was to raise awareness among the broader community. The final output of the exercise was a visual timeline of relevant global spaces where cybersecurity debates are taking place:

https://www.freedomonlinecoalition.com/wp-content/uploads/2015/05/Mapping-Brochure-WEB-1.pdf

In the public debate about how to provide security in the digital context, the dominant narrative has become increasingly entrenched pitting privacy and other human rights against public safety and national security. In practice, though, threats to privacy and other human rights can also harm public safety and security. This binary framing is therefore damaging to both sides of the equation, and creates antagonisms where mutual reinforcement is possible. Framing privacy and other human rights as antithetical to public safety and national security is not only misleading, but

undermines public safety and security, as well as freedom. Raising the profile of human rights protections in existing cybersecurity policy-making is necessary to offset this trend.

These recommendations are a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – that cyber security policies are rights respecting by design.

These recommendations were shared with the community in a successful workshop at the IGF in Brazil in 2015, the report for which can be found here:
https://www.intgovforum.org/cms/wks2015/index.php/proposal/view_public/18

The recommendations were also the subject of a session at RightsCon in March of 2016, the video for which can be found here:

https://www.youtube.com/watch?v=3IhlNEdpOks&index=10&list=PLprTandRM961m3pH%20sOlfij8wd9C_PHgqm

The final version of the recommendations will be presented at the 2016 annual meeting of the FOC meeting in Costa Rica October 16th and 17th

Segun Olugbile, Nigeria:

An Interagency network for collaboration has worked well for Nigeria. It involves policy synergy, cooperation, and collaboration among all government agencies thus evolving into a single point of contact and response on National Cybersecurity. The outcome produces a single corridor approach to engaging other non-government entities on partnership.

A Cybersecurity Nigeria mechanism spurred a cohesive approach on principles of engaging the whole of country's stakeholders. It provides a mechanism for building trust, engaging and uniting all stakeholders on common national cyber issues, through negotiation and understanding. This approach worked well during the development of Nigeria Cybersecurity Policy and Strategy 2013-2015.

APC:

The previously mentioned FOC WG1 is an example of best practice of multistakeholder collaboration on cybersecurity through its project on policy recommendations for human rights-respecting cybersecurity. Through multistakeholder dialogue, the working group developed a short document that can easily be used to evaluate existing cybersecurity processes as well as aid in the creation of new, more effective, human rights-enhancing cybersecurity policy[31].

Another example of a best practice is the Human Rights Protocol Considerations[32], one of 10 chartered research groups of the Internet Research Task Force, which is investigating whether standards and protocols can enable, strengthen or threaten human rights, as defined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. This unprecedented cross-sector work is building alignment between technologists and human rights advocates. Their outputs range from popular education tools about human rights and Internet standards to building awareness in various events of both the political and technical challenges to privacy.

---

[31] Freedom Online Coalition. (2015). Recommendations for human rights based approaches to cybersecurity. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf

[32] https://irtf.org/hrpc

FIRST:

Methods of enhancing cooperation and collaboration:

FIRST sees three high level areas of work ahead in ensuring CSIRT can cooperate more effectively both within their community, and beyond:

- Responding CSIRTs must be able to contact the partners they need to mitigate an attack. By themselves, CSIRTs, especially when they coordinate for more than a single constituent, do not always control computers and networks involved;

- When working with another team on an incident, both organizations must speak the same operational language and have accurate expectations on the use of the information provided.

- The community has the tools and techniques to enable automated information sharing. Analysts can focus on leveraging the information to truly understand the ramifications of the incident and make the right choices to reduce risk while mitigating the attack.

FIRST has invested in expanding the options of CSIRT when reaching out within their community. As an example, FIRST has initiated the Fellowship program, to allow new CSIRT with less financial capability to successfully join the community. In addition, FIRST has historically organized training, both developed by its partners and by itself, to ensure CSIRTs have a similar understanding of the issues at hand.

Finally, FIRST has convened its community to determine and publish a "CSIRT Services Framework" in the six official UN languages, which introduces a common understanding of the individual services offered by CSIRT teams.

Within its community, FIRST members have launched a number of working groups to standardize information exchange, focused on Vulnerability Coordination, the Traffic Light Protocol, and an Information Exchange Policy (IEP). FIRST also maintains the Common Vulnerability Scoring System (CVSS), which allows organizations to uniformly describe the impact of software vulnerabilities. While FIRST does not develop tooling for automated information exchange, our members leverage these standards in the development of their own tools.

There is an opportunity for the implementation of a similar approach between CSIRT and other stakeholders in the cyber security space. For instance, there are opportunities to train leaders in the Internet community who may not be security experts, on the issues and role of incident response teams, or how to best benefit from their work. In recent years, FIRST has contributed to the Internet Governance Forum and other governance efforts to create more awareness of the CSIRT community, its role and services. Other parties have also published guidance on the CSIRT community focused on other stakeholder groups, such as the Global Public Policy Institute and New America Foundation. Focused CSIRT assisting very specific groups, such as Access Now, have also exposed incident response capability to previously unserved audiences.

Identifying the right partner for cooperation:

Within our community, FIRST has long maintained its member database, a public resource for individuals to find a CSIRT and the constituency they are authoritative for. In 2015, FIRST opened up this data set through a well-structured Application Programming Interface. Network operators can leverage this tool to, in an automated manner; establish who to report a security incident to. FIRST is actively working with peer organizations in the community to extend the database beyond FIRST membership.

A well understood issue is that not every network is covered by a CSIRT. It is important for countries to support or establish a "CSIRT of last resort", which is willing to help coordinate across cultural and language barriers even if it has no official authority over the network in question to help address these gaps.

Corporations and software vendors which develop products have also increasingly stood up Product Security Incident Response Teams (PSIRT). These are increasingly part of the CSIRT community, and have a valuable role to play as the security response experts on the respective products they produce, which are increasingly becoming connected.

Contribution from the Geneva Internet Platform/DiploFoundation[33]:

Today's headlines often feature the word 'cyber', reporting on threats related to the virtual world: online child abuse, stolen credit cards and virtual identities, malware and viruses, botnets and denial-of-service attacks on corporate or government servers, cyber-espionage, and cyber-attacks on critical infrastructure including nuclear facilities and power supply networks.

Cybersecurity came into sharper focus with the rapid expansion of the Internet's user base. The Internet reiterated the old truism that technology can be both enabling and threatening. What can be used to the advantage of society can also be used to its detriment. One side effect of the rapid integration of the Internet in almost all aspects of human activity is the increased vulnerability of modern society. The Internet is a part of the critical global infrastructure. Other core services of modern society, such as electric grids, transport systems, and health services, are increasingly dependent on the Internet. They are frequent targets of cyber-attacks.

What are the real cybersecurity challenges? What is the role of diplomacy, international legal instruments, and regional and national policies in addressing these threats, and how efficient are they? How does international cooperation in cybersecurity work, and what are the roles of the various stakeholders?

Diplo focuses on these and other related questions through online and *in situ* courses, awareness-raising sessions and events, evidence-based analysis, policy research, illustrations, and videos and other visuals. At the same time, the *GIP Digital Watch* observatory, operated by DiploFoundation, maintains regular updates on cybersecurity issues, actors, processes and mechanisms.

- ***What are some examples of best practices in 'Cyber security Situational Awareness' where different organizations have worked together, specifically with law enforcement agencies and other specialists?***

NCSC-FI:

- We have many good examples of companies warning each other of malware campaigns, DDoS campaigns or giving tips (do's and don'ts) to their peers.
- If, for example, a certain organization finds out about malware campaign targeting the organization, it may send the information concerning the suspected malware to other organizations (including us) in its cooperative network. If needed, we will then use that same information, anonymize the target organization(s) and send an email etc. to other cooperative networks as well.

Fojon Kosta, Albania:

[33] https://issuu.com/diplo/docs/cybersecurity_executive_summary

A very good example is the collaboration and cooperation of the Albanian CIRT with State Police related and Albanian Governmental institutions and authorities. Another example is the cybersecurity cooperation between the National Bank of Albania and private banks in the country.

Segun Olugbile, Nigeria:

Nigeria's foremost coordinator of all security organizations, i.e. Office of National Security Adviser (ONSA) mobilizes all security and para-security organizations including the Military, Police, and other law enforcement agencies, through the Interagency network framework, into the Cybersecurity Nigeria forum.

OAS:

The Program has staged in collaboration with the South School of Internet Governance, 'SEGURINFO' in several of our member states. SEGURINFO is an annual meeting for information security, including intensive information sessions and networking for information security professionals and industry suppliers. The OAS is also a signatory to and promotes the STOP.THINK.CONNECT messaging convention. STOP. THINK. CONNECT. is a global online safety awareness campaign aimed at helping people to stay safer and more secure online. The message was created through a coalition of private companies, non-profits' and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG). Many countries and private sector entities have joined this initiative[34]. In October every year, the OAS Cyber Security Program organizes an event dedicated to raising public awareness about staying secure online in partnership with several organizations, such as the National Cyber Security Alliance, the US Department of Homeland Security, and the STOP.THINK.CONNECT.

Part III: Summary of 2016 BPF Dialogue/Contributions *(including discussions in the lead up to IGF 2016 and during dedicated substantive BPF session at IGF 2016)* and recommendations for way forward:

The following statements/messages from draft 1.0 of the output document found some general consensus amongst participants in the 2016 BPF:

- The involvement of government, private sector, civil society and other stakeholders in handling cybersecurity was stressed as fundamental in terms of sharing best practices, sharing results of critical assessments and identifying globally accepted standards of cybersecurity. All stakeholders must understand, respect and trust each other's expertise and competences.
- It was emphasized that to many today, the word "cybersecurity" is often loaded with context, and many organizations associate it with government decision making, or commercial security solutions. Within the IGF, it was said, there is an opportunity to redefine cybersecurity as a common goal between all stakeholders, and to work towards finding a common understanding about what productive cooperation and collaboration might look like.
- It was said that the term "cybersecurity" can mean very different things to different stakeholders depending upon the context in which it's being used. (national security; public security; enterprise security; incidence response; personal security; protection against large scale data breaches and cyber-crime/online crime; uncertainties about how our data is being used; surveillance and other online threats, etc.)

[34] https://www.stopthinkconnect.org/

- There was broad agreement that the roles and responsibilities of stakeholders are evolving in making the Internet a secure and safe place for people to socialize and conduct business. It is clear that security is no longer just the purview of governments and that it is increasingly a multistakeholder imperative.
- Evolving understandings of cybersecurity make efforts to ensure the Internet is a secure and safe place an important focus of policy that requires input from multiple stakeholders. Starting from a dominant technical perspective of cybersecurity and focusing on protecting information infrastructure, debates around cybersecurity have rapidly broadened, bringing in many issues from cybercrime to secure access policies to data ethics and human rights under its banner.
- There was general consensus within the BPF around the notion that cybersecurity initiatives should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users.
- It's imperative to promote more robust, effective and timely information-sharing, cooperation and coordination among cybersecurity stakeholders at the national, regional and international levels. Cooperation and collaboration is important in cybersecurity, not only to avoid duplicate work and analysis, but also in respect to less mature entities, being able to profit from the experience and expertise of others and as such develop faster thereafter.
- Within the CSIRT community, automating information exchange where possible, and ensuring CSIRT's ability to process information at an increasing pace is extremely important. CSIRT's can often be resource constrained in terms of qualified analysts, and allowing them to focus on harder problems that require expert review is critical. However, it is important to clarify that prior to any automated exchange taking place, it is crucial for stakeholders to set expectations around how the data will be used. Sharing indicators may not be helpful if they are not used correctly, or are used for different purposes than intended. While there are typically many technical means of addressing a security incident, it is most important that goals are aligned and expectations are clearly set.
- For CSIRTs to effectively work with each other, or other peers within the community, trust is a crucial requirement. Trust is typically not established through legal agreements, but through a history of working with each other. Developing trust is easiest when the objectives of both organizations align. When both organizations have as goal to remediate the incident and restore operations, they both see value in the information exchange.
- There is a need for more civil society involvement in cybersecurity debates in all countries, and in particular in developing countries. Furthermore and in parallel with increased participation, more opportunities for education and awareness raising among civil society groups on issues of cybersecurity should be supported. For cybersecurity cooperation and collaboration to be enhanced globally – and particularly in global south countries – the first step is to create a level playing field in terms of knowledge, skills and capacity for engagement.

IGF 2016 dedicated BPF session (8 December 2016)

View the transcript here: https://www.intgovforum.org/multilingual/content/igf-2016-–-day-3-–-room-9-bpf-cybersecurity

Watch the webcast of the session here:
https://www.youtube.com/watch?v=P1cxUnimmFQ&t=579s

Chair(s) and/or Moderator(s) and Speakers/Discussants:

Markus Kummer, Coordinator for 2016 IGF BPF Cybersecurity (Chair)

Segun Olugbile, Co-Coordinator for 2016 IGF BPF Cybersecurity

Maarten Van Horenbeeck, Fastly, FIRST (Moderator)

Panel:

Richard Leaning, RIPE NCC (Speaker)

Isabel Skierka, Digital Society Institute (DSI) (Speaker)

Kerry-Ann Barrett and Barbara Marchiori, Organization of American States (OAS) (Speakers)

Grace Githaiga, KICTANet (Speaker)

Matthew Shears, Freedom Online Coalition (FOC) (Speaker)

Hiroshi Esaki, Graduate School of Information Science and Technology, The University of Tokyo (Speaker)

Some suggestions for themes/topics for the BPF Cybersecurity in 2017 were:

- Security awareness best practices
- User knowledge gaps
- Child online protection and online safety
- Frameworks on cybersecurity
- Regional and global cybersecurity cooperation
- Civil-society and government cooperation
- Transparency of private sector cybersecurity policies –
- Best practices for contractual arrangements with information security services
- Mechanisms to improve multi-stakeholder cooperation in formulating and implementing national cybersecurity goals
- Development and cybersecurity concerns
- How can cybersecurity contribute to Sustainable Development Goals
- Need for embedded security as broadband expands

Annex I

List of Contributions

- **Contribution from the Freedom Online Coalition Working Group 1 - "An Internet Free and Secure"**
- **Contribution from Mr. Fojon Kosta, Government of Albania Contribution from Mr. Fojon Kosta, Government of Albania**
- **Contribution from Mr. Olusegun H. Olugbile, Member National (Nigeria) Advisory Council on Cybercrime**
- **Contribution from the Geneva Internet Platform (GIP)/DiploFoundation: *Cybersecurity Competence Building Trends* - http://www.diplomacy.edu/ig/cybersecurity (*the links to the full report and the illustrated executive summary, versions for download and for review*)**
- **Contribution from the Nigeria IGF (NIGF)**
- **Contribution from Mr. Jerome Athias: https://www.helpnetsecurity.com/2016/07/13/security-vendor-collaboration/**
- **Contribution from Mr. Shreedeep Rayamajhi, Razynews**
- **Internet Governance Capacity Survey: Nepal (Submitted by Mr. Shreedeep Rayamajhi)**
- **Contribution from the Internet Society (ISOC): *A policy framework for an open and trusted Internet* – http://www.Internetsociety.org/doc/policy-framework-open-and-trusted-Internet**
- **Contribution from the Internet Society (ISOC): *Collaborative security approach to tackling Internet security* issues – http://www.Internetsociety.org/collaborativesecurity**
- **Contribution from the Association for Progressive Communications (APC)**
- **Contribution from The Information Technology - Information Sharing and Analysis Center (IT-ISAC)**
- **Contribution from the Organization of American States (OAS)**
- **Contribution from the Forum of Incident Response and Security Teams (FIRST)**
- **Contribution from Global Partners Digital**
- **Contribution from the National Cyber Security Centre - Finland (NCSC-FI)**
- **UNODC Cybercrime Repository**

- **Contribution from Mr. Peter Cassidy - Cybersecurity Baselining Protocol**