IGF 2017
Best Practice Forum on Cybersecurity

Editor Wim Degezelle

January 2018

IGF 2017 - Best Practice Forum on Cybersecurity

Table of contents

IGF 2017 - Best Practice Forum on Cybersecurity

Table of contents 2

Executive summary 4

Part I: Framing the 2017 IGF Best Practice Forum Cybersecurity 6

Introduction 6

The 2017 BPF Cybersecurity: purpose and outline 7

Methodology & community input 7

Part II: Cybersecurity as an enabler of development 9

Section 1: Cybersecurity's ability to support the SDGs 9

1.1. Trust and Confidence in ICTs and the Internet 9

1.2. The impact of poor cybersecurity 9

1.3. The different faces of cybersecurity 10

Section 2: Policy options to mediate cybersecurity threats 12

2.1. Mediating threats that undermine the contribution to achieving the SDGs 12

2.1.1. Introduction - CENB and SDGs 12

2.1.2. An analysis of the CENB & SDG cybersecurity implications 13

2.1.3. Policy options to help address the CENB cybersecurity challenges 13

2.1.4. Additional concerns and challenges 19

2.2. Defining responsibilities for the stakeholder communities 20

2.2.1. Multistakeholder cooperation on cybersecurity - a shared responsibility 20

2.2.3. Stakeholder communities and their responsibilities 21

Section 3: Areas to develop further stakeholder conversation 25

Part III: Conclusions and way forward 29

Annexes 31

Annex 1: Contributions to the 2017 BPF Cybersecurity 31

Annex 2: CENB Phase I & II Cybersecurity-focused policy analysis 32

CENB Phase II - Cybersecurity-focused policy analysis 32

CENB Phase I - Cybersecurity-focused policy analysis 33

Annex 3: Report of the BPF Cybersecurity session at the 2017 IGF meeting 40

Annex 4: Summary of the BPF Cybersecurity coordination session at the 2017 IGF meeting 43

Executive summary

The Best Practice Forum (BPF) on Cybersecurity is part of the 2017 intersessional work programme of the Internet Governance Forum (IGF). The BPF aims to provide a broad multistakeholder platform for engagement on cybersecurity matters. This BPF's output document is part of the tangible outcome of the 2017 IGF.

The BPF on Cybersecurity was conceived in 2016 as a multi-year project that grew out of and builds upon the work of the BPF on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet security and the BPF on Regulation and Mitigation of Unsolicited Communications, both of which ran during 2014 and 2015.

The 2017 BPF explored how cybersecurity influences the ability of ICTs and Internet technologies to support the achievement of the SDGs, it looked at the roles and responsibilities of the different stakeholder groups, and aimed to identify options for policy mitigations that could help ensure that the next billion(s) users can be connected in a safe and reliable manner and fully benefit from existing and future technologies. The BPF collected community views on what critical cybersecurity issues would benefit from further multi-stakeholder approach.

The BPF Cybersecurity focused on development and used previous IGF work – the IGF Policy Options for Connecting and Enabling the Next Billion(s), Phase I and II (CENB I and CENB II) – as starting point to identify a set of security challenges and discuss how to mitigate the risks.

> The BPF's cybersecurity analysis of the IGF CENB policy options identified a set of 10 security challenges:
>
> 1. Securing the reliability of and access to Internet services;
> 2. Securing the mobile Internet;
> 3. Protecting against potential abuse by authorities;
> 4. Confidentiality and availability of sensitive information;
> 5. Fighting online abuse and gender-based violence;
> 6. Securing shared critical services and infrastructure supporting access;
> 7. Vulnerabilities in Industrial Control Systems (ICS) technologies;
> 8. Preventing collected information from being repurposed;
> 9. Deploy secure development processes;
> 10. Prevent unauthorized access to devices.

Six additional policy areas were raised in individual contributions:

1. Awareness building and capacity development;
2. Supporting cyber resiliency of cities;
3. Lack of diversity in cybersecurity;
4. Cryptocurrency;
5. Impact of social media on cybersecurity;
6. Whistleblower policies and implementation.

Via a public call for input and outreach to National and Regional IGF initiatives, the BPF collected suggestions on how to deal with these cybersecurity challenges. The BPF received 27 formal contributions, input via its open maling list and its virtual meetings, and during the BPF Cybersecurity Workshop organised at 2017 IGF Meeting in Geneva. These suggestions have been consolidated per security risk and can be found in section 2.1.3 and 2.1.4 (pages 13 to 20) of the report.

The BPF's policy suggestions are intended to inspire policy decision makers by providing different ways to face and tackle cybersecurity challenges.

In addition to its focus on security challenges originating from the CENB recommendations, the BPF also collected community input on what other (new) areas and issues could potentially benefit from a multistakeholder approach. This topic was one of the key questions discussed at the two session BPF Cybersecurity sessions during the 2017 IGF Meeting in Geneva. A non-exhaustive overview of areas to develop further stakeholder conversation can be found in section 3 (page 25 to 28). Some of the issues are already been dealt with by one or more stakeholder groups in specific forums. Where this is the case, one should be wary of creating new venues that duplicate the work, and look for opportunities to establish dialogue and cooperation among forums. Interested stakeholders are advised to consider joining the existing forums and so further develop multistakeholder dialogue on the issue(s) at stake.

At the 2017 IGF Meeting in Geneva, the BPF Cybersecurity started an exchange to get guidance from the community on possible topics and directions for further work of the BPF on Cybersecurity. This community feedback was to feed into a proposal to the IGF MAG to consider a continuation of the BPF on Cybersecurity in 2018.

Acknowledgements

This BPF output document is the result of a collaborative effort of many.

We would like to recognise the MAG for selecting cybersecurity as topic for a BPF as part of the 2017 intersessional work program; the BPF Co-Facilitators Mr. Markus Kummer and Mr. Olusegun Olugbile and the BPF Lead-Expert Mr. Maarten Van Horenbeeck for their guidance and leadership; the numerous contributors and active participants to the BPF discussions on the mailing list, during virtual meetings and at the BPF sessions during the IGF Meeting in Geneva for their involvement, input and feedback; the panellists on the IGF Workshop; all who contributed to the content of this document by submitting formal contributions; and the IGF Secretariat, Ms Eleonora Mazzucchi and Mr. Wim Degezelle for providing support to the BPF and holding the pen on this output document.

Part I: Framing the 2017 IGF Best Practice Forum Cybersecurity

Introduction

The Best Practice Forum (BPF) on Cybersecurity is part of the intersessional work programme feeding into the 12th annual meeting of the Internet Governance Forum (IGF) held in Geneva, Switzerland from 18 to 21 December 2017.

The BPF aims to both provide a broad multistakeholder platform for engagement on cybersecurity policy matters, which increases existing cooperation and builds new synergies amongst cybersecurity initiatives and processes, and to contribute to a richer and more tangible output of the IGF[1]. The BPF Cybersecurity fits well under the overall theme of the 2017 IGF, *Shape Your Digital Future!* .

The BPF on Cybersecurity grew out of the BPF Establishing and supporting Computer Security Incident Response Teams (CSIRTs) for Internet security, and the BPF Regulation and Mitigation of Unsolicited Communications, both of which ran during 2014 and 2015.[2]

As an outcome of both groups, it was identified that the topics they had tackled were somewhat limiting, and there was no existing forum within the intersessional work to discuss other cybersecurity related challenges and to approach cybersecurity in a more holistic manner. In addition, it was said that "cybersecurity" as a term was ill defined within our community, and could benefit from deeper investigation and definition.

In 2016, the first Best Practices Forum on Cybersecurity hence started off with discussions enabling participants to understand the wider context of the word "cybersecurity" for each stakeholder group. The BPF made it clear right from the beginning that this work needed to be conceived as a multi-year project. It then worked to:

- Identify the communications mechanisms between stakeholder groups to discuss cybersecurity issues;
- Understand the typical roles and responsibilities of each group in making sure the Internet is a secure and safe place;
- Identify common problem areas in cooperation, and good best practices for doing so.

A set of 10 conclusions was drawn, which broadly echoed multi-stakeholder cooperation as critical, and put particular stress on how stakeholders should understand, respect and trust each other's expertise and competences. The final outcome of the 2016 BPF on Cybersecurity can be found on the IGF web site [3].

[1] The BPF intends to enrich the IGF output *'to enhance the impact of the IGF on global Internet governance and policy'* as called for in the report by the UN General Assembly Economic and Social Council (ECOSOC)

[2] BPF archived content: https://www.intgovforum.org/multilingual/content/bpf-archived-content .

[3] 2016 BPF on Cybersecurity, *'Building Confidence and Security in the Use of Information and Communications Technologies (ICTs) through Enhanced Cooperation and Collaboration',* http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3405/453 .

The proposal[4] for the 2017 BPF Cybersecurity was approved by the IGF's Multistakeholder Advisory Group (MAG) on 11 April 2017[5]. The BPF's intersessional discussions culminated in the BPF Cybersecurity workshop at the 12th IGF meeting in Geneva and this BPF document was published as part of the official output of 12th IGF meeting.

The 2017 BPF Cybersecurity: purpose and outline

The Best Practice Forum on Cybersecurity realized that making Internet access more universal, and thus it supporting the United Nations Sustainable Development Goals (SDGs)[6], has significant cybersecurity implications. Well-developed cybersecurity helps to create an enabling environment for information and communications technoligies (ICTs) and Internet technologies to contribute to meeting the SDGs. Poor cybersecurity can reduce the effectiveness of these technologies, and thus limit the opportunities to help achieve the SDGs.

The 2017 BPF explored how cybersecurity influences the ability of ICTs and Internet technologies to support the achievement of the SDGs, it looked at the roles and responsibilities of the different stakeholder groups, and aimed to identify options for policy mitigations that could help ensure that the next billion(s) users can be connected in a safe and reliable manner and fully benefit from existing and future technologies. The BPF collected community views on what critical cybersecurity issues would benefit from further multi-stakeholder approach.

This BPF output is the product of a bottom-up, open and iterative process to which all stakeholders were invited to participate. The main steps and methodology are briefly described in the next section.

Methodology & community input

The approval of the project proposal for BPF Cybersecurity by the 2017 MAG kicked off the BPF's open and iterative process[7]. The BPF Cybersecurity convened regular virtual meetings open to all interested stakeholders and discussed progress on an open mailing list. Draft versions of the output document were posted for community comment on the IGF website and presented at a dedicated workshop during the 2017 IGF meeting in Geneva.

[4] Proposal for 2017 Best Practice Forum (BPF) on Cybersecurity, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/625 .

[5] 11 April 2017 MAG Virtual Meeting, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3813/581 .

[6] https://sustainabledevelopment.un.org

[7] The process is documented on the IGF website, https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1 .

The BPF Cybersecurity launched a *call for contributions*[8] to collect substantial community input on the BPF's subject matter. Drawing primarily from an analysis of the potential cybersecurity implications of the policy suggestions for enabling connectivity and supporting the SDGs, formulated by the *IGF Policy Options for Connecting and Enabling the Next Billion(s)*[9], the BPF invited community input on how to mitigate these challenges.

In addition, the BPF asked the community to identify responsibilities of the different stakeholders for mitigating risks, and to weigh in on what critical cybersecurity issues would benefit from a further multistakeholder approach.

The BPF made special effort to seek input from National and Regional IGF Initiatives (NRIs) via outreach and an NRI-specific questionnaire.

This output document combines the input the BPF received from 27 formal contributions[10], input via its open maling list and its virtual meetings, and during the BPF Cybersecurity Workshop organised at 2017 IGF Meeting in Geneva.

[8] A questionnaire was distributed via the IGF website, BPF mailing lists, to contributors to earlier BPFs and by targeted outreach. The questions were made available in English and Spanish. A dedicated questionnaire was used to seek input from National and Regional IGF initiatives (NRIs).

[9] IGF Policy Options for Connecting and Enabling the Next Billion(s), https://www.intgovforum.org/multilingual/content/igf-policy-options-for-connecting-and-enabling-the-next-billions .

[10] The contributions are listed in annex 1 and archived on the IGF website.

Part II: Cybersecurity as an enabler of development

Section 1: Cybersecurity's ability to support the SDGs

Substantial input for this section was generated from the responses to the BPF’s call for contributions, and in particular the responses to the questions:

> *‘How does good cybersecurity contribute to the growth of and trust in ICTs and Internet technologies, and their ability to support the SDGs?’*
>
> *‘How does poor cybersecurity hinder the growth of and trust in ICTs and Internet technologies, and their ability to support the SDGs?’*

1.1. Trust and Confidence in ICTs and the Internet

‘The Internet needs a solid foundation in trust for its full potential to be realized.’[11] Well-developed cybersecurity contributes to building trust and feeds the confidence in ICTs and Internet technologies enabling them to become instruments used by people and organisations in pursuing their goals.

‘Civil and political rights are clearly boosted by Internet access, but the Internet also positively impacts economic development when societies can trust in Internet-connected systems and robustly interact, and transact online.’[12] Good cybersecurity stimulates growth in users and usage of Internet technologies, which help to accelerate business, make economies grow and increase the wealth that becomes available for distribution. They contribute to the reduction of transaction costs, increase transparency and accelerate knowledge and information transfer. Good cybersecurity stimulates the use of technologies that have the potential to contribute to achieving the SDGs.[13]

In short, cybersecurity helps to build the confidence needed to motivate the use of ICTs and the Internet technologies, and the SDGs drive that energy towards achieving the goals to end poverty, protect the planet and ensure prosperity for all.[14]

1.2. The impact of poor cybersecurity

Poor cybersecurity threatens the growth of ICTs and Internet technologies. Poor cybersecurity exposes organisations and individuals to risks and attacks, and opens doors for ill-meaning parties to spy on actors or meddle with democratic affairs. In a more indirect way, a perception of insecurity creates distrust in ICTs and the Internet and a diminishing

[11] BPF contribution the Internet Society.
[12] BPF contribution Access Now
[13] BPF contribution Caribbean IGF, BPF contribution Mohit Saraswat
[14] BPF contribution Shredeep Rayamajhi

adoption of new technologies. Poor cybersecurity will reduce the use and effectiveness of these technologies, and thus limit the opportunities to help achieve the SDGs.[15]

'Poor cybersecurity hinders growth and trust in ICTs as it leads to lack of confidence in online systems and services, thus discouraging investment and usage. A lack of cyber hygiene increases vulnerability to cyber attacks and reduces the ability to effectively respond to and recover from cyber incidents which in turn promotes a lack of trust in the digital economy.'[16] Where poor cyber security enables cyber espionage, the loss of industrial, military, policy and academic development, research and knowledge can have important implications.[17]

1.3. The different faces of cybersecurity

Cybersecurity is a broad concept that covers many aspects. Some argue that one definition is impossible as cybersecurity means too many different things depending on the context. The 2016 BPF dedicated time to a discussion on different definitions of the term 'cybersecurity'. The highlights of this exchange can be found in the output document of the 2016 BPF Cybersecurity[18].

ICTs and Internet technologies increasingly underpin society, economy, and policy. Cyberspace faces new challenges such as security and stability, infringement on privacy and intellectual property, cyber terrorism and cyber surveillance activities.[19] The submissions to the BPF reflect different expectations, priorities, and perspectives on how cybersecurity can contribute to the growth and trust in ICTs and Internet technologies, and their ability to support achieving the SDGs. This sections aims to give an overview of the different 'faces' of cybersecurity.

Infrastructure

The Internet is a network of networks and the ability to resist cyberattacks is only as strong as its weakest link.[20] Sustainable development of all levels is directly related to the protection of all aspects of this infrastructure, including security.[21]

One contribution introduced the concept of a "*public core*" which is worthy of protection. This core of the Internet encompasses two elements: '(i) a clearly distinguishable "*inner core*" which consists of the core functionality underpinning the Internet (in particular the forwarding and naming functions and infrastructure of the Internet and those actors

[15] BPF contribution Microsoft, BPF contribution IGF Mauritius
[16] BPF contribution Commonwealth Telecommunications Organisation (CTO)
[17] BPF contribution Wout de Natris
[18] 2016 IGF BPF on Cybersecurity, *'Building Confidence and Security in the use of Information and Communications Technologies (ICTs) through Enhanced Cooperation and Collaboration'*, http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3405/453
[19] BPF contribution China
[20] BPF contribution Microsoft
[21] BPF contribution Mobile Communication Company of Iran (MCI)

responsible for their day to day management), and (ii) a less clearly distinguishable "*outer core*" of potentially critical functionality, whose impact on the overall stability and security of the Internet as a whole may be uncertain, or which may fluctuate depending on circumstances.'[22]

Trade, commerce, industry and production

'Good cybersecurity is a means of achieving and sustaining the credibility of the Internet as a safe environment for businesses to thrive and sustain economic value.'[23] Effective cybersecurity is essential 'to engage fully in the increasingly cyber-dependant trade and commerce. Robust cybersecurity frameworks enable individuals, companies and nations to realise the full potentials of the cyberspace, without fear or reservation, promoting cross-border delivery of services and free flow of labour in a multilateral trading system.'[24]

Cyber attacks, vulnerabilities and security breaches break trust of businesses online, which directly impacts productivity and economic growth in developing countries where ICTs are more adopted for the delivery of services.[25] Also the small and medium enterprises (SMEs) face the challenge to secure themselves from cyber attacks and to promote confidence and trust in their online services.[26]

Privacy/Data protection

Good cybersecurity policies, practices and legislation put people and their rights at the centre. They protect individuals, their data, devices and networks, and foster trust, stability and confidence in ICTs. Poor cybersecurity results in vulnerabilities and data breaches are catastrophic for privacy and undermine trust in digital developments. Many countries have insufficient or no legislation that protects data.[27]

Technology can be an enabler of all SDGs, but must be secure. Relying heavily on ICTs and the Internet to implement large scale development projects without strong cybersecurity in place leaves some of the world's most vulnerable people vulnerable in a new way, for example when their sensitive personal information such as biometrics or health data is not sufficiently well protected.[28]

Human Rights, Rule-of-law and Democracy

Good cybersecurity contributes to the 'protection of human rights, democracy and rule of law.'[29] Certain security measures, however, might as well pose a serious threat to these democratic values, in particular where governments are increasingly asserting control over

[22] BPF contribution Global Commission on the Stability of Cyberspace (CGSC).
[23] BPF contribution Opeyemi Onifade (AfICTA)
[24] BPF contribution Commonwealth Telecommunications Organisation (CTO)
[25] BPF contribution Internet Policy Observatory Pakistan
[26] BPF contribution Commonwealth Telecommunications Organisation (CTO)
[27] BPF contribution Privacy International
[28] BPF contribution Association for Progressive Communication (APC)
[29] BPF contribution Council of Europe Cybercrime division

the Internet and stigmatize security measures, such as encryption.[30] 'Cybersecurity and human rights are complementary, mutually reinforcing and interdependent.' To avoid that cybersercurity policies have a negative impact, they should incorporate human rights by design[31], States should work together to curb trade of spyware, respecting human rights[32], and actively participate in discussion forums with the other stakeholders[33].

Poor cybersecurity and information breaches might, for example, have an impact on the ability of civil society to campaign against political decisions or weaken the voice of activists.[34]

Section 2: Policy options to mediate cybersecurity threats

2.1. Mediating threats that undermine the contribution to achieving the SDGs

2.1.1. Introduction - CENB and SDGs

The IGF work on *Policy Options for Connecting and Enabling the Next Billion(s)* (CENB) is a multi year work programme aiming to develop comprehensive sets of policy recommendations based on broad consultations, bottom up crowdsourcing and cross-engaging the work of the different intersessional work tracks and IGF initiatives.

The first phase in 2015 (CENB I)[35] focussed on infrastructure, increasing usability, enabling users, entering affordability and enabling environments. The subsequent phase in 2016 (CENB II)[36] discussed how ICTs can help reach the United Nations SDGs. The ongoing CENB III[37] in 2017 narrowed its scope to focus on a limited number of SDGs impacted by ICTs.

The 2017 BPF Cybersecurity builds upon the community work of CENB I and II, and established cross-fertilisation with CENB III, in particular with the CENB discussions related

[30] BPF contribution Access Now
[31] BPF contribution Association for Progressive Communication (APC), quoting from 2015 Freedom Online Coalition 'Recommendations for human rights based approaches to cybersecurity'
[32] BPF contribution Access Now
[33] BPF contribution Wout de Natris
[34] BPF contribution Luisa Lobato
[35] CENB I output document: http://www.intgovforum.org/multilingual/content/connecting-and-enabling-the-next-billion-phase-i
[36] CENB II output document: https://www.intgovforum.org/multilingual/content/igf-2016-policy-options-for-connecting-and-enabling-the-next-billions-phase-ii
[37] CENB III webpage: https://www.intgovforum.org/multilingual/content/policy-options-for-connecting-and-enabling-the-next-billions-—-phase-iii-call-for-public

to SDG Goal 9: ‘Build resilient infrastructure, promote sustainable industrialization and foster innovation’.

2.1.2. An analysis of the CENB & SDG cybersecurity implications

The BPF performed a cybersecurity assessment of the CENB output documents to identify potential risks and security challenges emerging from the CENB policy recommendations. The detailed analysis of the CENB cybersecurity implications can be found in annexes to this report. The CENB II analysis dives deeper into the connection between risks and the SDGs. For this section, the BPF focused in particular on the CENB II recommendations, because of their direct link to the SDGs.

The BPF identified a list of 10 potential threats and cybersecurity challenges emerging from the CENB II policy recommendations:

a. Denial of Service attacks and other cybersecurity issues that may impact the reliability and access to Internet services;
b. The security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments or self-identification;
c. Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended;
d. The confidentiality and availability of sensitive information, in particular in medical and health services;
e. Online abuse and gender-based violence;
f. Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS) and Internet Exchange Point (IXP) communities;
g. Vulnerabilities in the technologies supporting industrial control systems (ICS);
h. The use and repurposing of information collected for a particular purpose, for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data;
i. The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis;
j. Unauthorized access to devices that play an increasingly important role in people's daily lives.

2.1.3. Policy options to help address the CENB cybersecurity challenges

The BPF discussed the 10 identified cybersecurity challenges originating from the CENB policy options (see 2.1.2) to find ways to mitigate the risks. This led to a list of policy suggestions to help address each of the challenges.

Substantial input for this section was generated from the feedback on the call for contributions, and in particular from the responses to the question *‘Do you see particular* *policy options to help address CENB risks?'.* This delivered a long list of policy suggestions that were subsequently discussed and consolidated. They are shown below. A number of additional concerns and challenges that emerged during the discussions, are added in section 2.1.4.

When reviewing any policy option, participants to the BPF flagged that the following criteria should be taken into account:

- *Does the policy option provide the right incentive for the correct security controls to be implemented?*
  In cybersecurity, the one implementing the security control is often not the one that sees the benefit. For instance, when deploying a technical measure such as filtering spoofed packets, the implementer is preventing their network from attacking others, rather than directly seeing benefit. The value is in all networks implementing the measure, which protects the community.
- *Can the policy be implemented through a best practice, rather than regulation?*
  For instance, governments are large technology buyers, and may be able to influence device makers to implement security controls by requiring them from a vendor. This may be more effective than an outright rule requiring those same controls, that may be difficult to implement.
- *Does the new rule have unforeseen consequences?*
  For instance, requiring data to remain within the border of a country may cause costs to go up, and cause interconnects to happen outside the country entirely. Organizations tend to respond to cost incentives, so hard rules may move security risks outside of the borders of the country, rendering other national policies less effective.

Policy options to help address the CENB cybersecurity challenges

What follows is an non-exhaustive set of policy suggestions that is expected to evolve over time rather than being a fixed and detailed checklist. The list of policy suggestions reflects the input and experiences of the many contributors to the BPF and intends to inspire policy decision makers by providing ways to face and tackle cybersecurity challenges. Policy makers should grab the ideas to further develop them within the context of their own organisations, fields or countries, and where relevant.

a. **Securing the reliability of and access to Internet services**
   i. Technical community members could be incentivized to develop tools and standards to identify and appropriately hold accountable cyber criminals.
   ii. Preferably, priority is given to technical solutions to prevent cyber attacks, prior to other policy such as criminalisation. A good flow and exchange of solutions to find, mitigate and address vulnerabilities is key.

iii. Governments are encouraged to identify and implement international conventions to address cybercrime, and provide a legal framework for investigation, prosecution and sanctioning. This offers means to criminalize and prosecute cybercrime.

iv. The promotion of technologies for small and medium enterprises (SMEs) to secure themselves from cyber attacks would contribute to the confidence and trust in their online services.

v. Perpetrators of DDoS attacks should be held accountable through technical identification and criminal investigation of attacks. Warnings of DDoS, such as ransom demands, should be quickly disseminated through the network of security practitioners.

vi. Software and product vendors should be advised to implement security at all stages of the development lifecycle. Products should be patched to address vulnerabilities throughout a well defined lifecycle. This lifecycle should take into account interactions with other software. For instance, it's advisable that developers not create situations where software is only supported on hardware or an operating system which is no longer supported by its respective vendor.

vii. Support technical measures to enhance resiliency of networks and promote access.

viii. A shift in the mindset of the tech and software industry that recognises customers as such and stop seeing and treating them as users, would change dependency roles and put responsibility for (ongoing) security of products with the manufacturer, who then becomes responsible for secure software at the start and for fixing software flaws in a timely manner, while the customer remains responsible for correct use within the law. The onus for realising a safer Internet becomes as such a shared responsibility.

ix. Communicated data for security monitoring in a unified format and language (a log in one tool should mean the same as a log in another tool), would allow systems to reliably identify genuine source and user of an event, and reduce the chance that perpetrators cannot be tracked. This would help all level of ISPs and Internet coordination bodies to better coordinate protocols to respond to malicious activity.

b. **Securing the mobile Internet**

i. The technical community should be encouraged to develop and research security solutions, and to raise awareness around mobile threats. Developers of mobile technologies should be encouraged to implement a secure development lifecycle. A minimum of built-in security features and capabilities should be implemented in systems.

ii. Mobile devices should be considered "computer systems" in applicable law, similar to the stipulations of the Budapest Convention.

iii. Gaps in understanding, between users and the product vendors, of security vulnerabilities should be avoided. Such gaps may arise from the wide variety of mobile devices, and for devices outside of their main support lifecycle.

iv. Repositories of security best practices for mobile apps, such as the detection of malicious applications, would be helpful. Mobile applications should use encryption technologies such as HTTPS when communicating over networks.

v. States could contribute by adopting data protection rules, such as Convention 108 of the Council of Europe.

vi. It's important that citizens and users have access to good instructions on how to manage their devices. Governments may need to support low income citizens to ensure that they have equal access to this level of support.

vii. Mobile operators should acknowledge that they are no longer simply a device reseller, but have taken on the role of being a software provider to end users. This implies that they should maintain, develop and deploy patches against a well documented life cycle for devices.

c. **Protecting against potential abuse by authorities**

i. Governments and intergovernmental organizations could speak out and criticize the use of technologies for abusive purposes by other governments.

ii. Surveillance undermines privacy and threatens freedom of expression. Legal and constitutional safeguards could help to minimize its impact on trust. Vigilance is advised to avoid that prioritizing surveillance weakens rather than strengthens security for all concerned.

iii. It's good practice to assure that criminal law measures are subject to law safeguards and conditions. These controls apply less to national security services for which stronger supervision and accountability may be needed.

iv. States are invited to support and promote an open Internet, safe and secure environment, and to consider regulation instead of censorship. Privacy and Data Governance policy/laws would be welcomed.

v. Ethics are an important part of a thriving cybersecurity community. Ethics standards should as much as possible be endorsed and promoted at all levels, within government, industry and society, and with regard to all technologies, including ICTs and IoT technologies.

d. **Confidentiality and availability of sensitive information**

i. Civil society could serve as a watchdog to closely observe when sensitive and confidential information is disclosed.

ii. Legal frameworks could help to address data security concerns, and impose security obligations for governments and companies. Reporting requirements for incidents would allow subjects to take actions to protect themselves from consequences, and assure that governments are made aware of risks and threats in their countries. States should take these rules also into account for their own data intensive projects

iii. Applications processing sensitive information should have secure baseline/applicable controls, and should be certified to ensure that this baseline is applied. Sensitive user data should only be made available on a "need to know basis".

iv. Availability of services with critical data pertaining to users should be monitored and managed.

v. All stakeholders could contribute to privacy by informing users when profiling takes place, and by providing audit trails as well as mechanisms to opt out of collection.

vi. There should be general acceptance that personal data is not owned by a company, but by the user. Transfer of account information to another entity should be managed using descript processes that involve consent. Privacy rules should equally apply to the mobile and app environment.

vii. Jurisdiction issues in the third world are often complex, as the user's data is generally hosted with foreign companies. The private sector and States should acknowledge this and consider measures that provide control to the user over his/her information.

e. Fighting online abuse and gender-based violence

i. States should consider to develop laws to deter online exploitation.

ii. Partnerships between all stakeholder groups could help to raise awareness of online abuse and gender-based violence, and support awareness building and education programmes and commit support resources.

iii. International rapid response teams could mitigate abuse across platforms and services, by tracking of abusers and fast-tracked responses. These processes should be global, and support an ombudsman or review process.

iv. Processes to remove content when appropriate should be defined in line with the law of the country. Technology providers should provide means of monitoring and law implementation.

v. States should fully implement CEDAW at the national level to respect, protect and fulfil women's rights, pursue a preventive and proactive approach to gender-based violence (GBV), and recognise GBV as a human rights violation.

vi. Gender-unequal access to technology and women's low presence in ICT could be confronted, through affirmative action and subsidies for ICT-related courses, or comprehensive capacity building. Companies should take a rights-based approach and adopt the Women's Empowerment Principles. Adequate budgets and resources should be allocated by States to address online GBV.

f. Securing shared critical services and infrastructure that support Internet access

i. States should be encouraged to implement cybersecurity frameworks such as the US NIST Cybersecurity framework and associated laws.

ii. The technical community should be encouraged to implement DNSSEC, RPKI and other key security technologies with the help of other stakeholders. States could help by supporting the technical community to work on ccTLD capacity building, IXP services and resiliency development. Protecting these resources is critical, requires a multistakeholder approach and acknowledgement of global interest.

g. **Vulnerabilities in the technologies supporting industrial control systems**

   i. Vulnerabilities should be urgently addressed by the technical community.

   ii. It is good practice for States and operators of industrial control systems to include disaster preparedness and response, and business continuity planning in operations.

   iii. The technical community and operators should leverage common language and sound security practices in current standards.

   iv. States and other stakeholders should support the development and sharing of security practices for ICS such as identifying vulnerabilities, and ensure patches are available. ICS cybersecurity in developing countries requires special attention.

   v. Operational responsibility should be defined and technology developers should be hold accountable for addressing security vulnerabilities.

   vi. States and private sector should question what SCADA and other control systems need an Internet connection and what systems are better kept offline or be disconnected from the Internet in order to be more secure.

h. **Preventing collected information from being repurposed for other, inappropriate purposes.**

   i. Management of information is critical. Companies should develop controls for safeguarding the information.

   ii. States could enact appropriate laws to criminalise use of information beyond its intended, appropriate purpose.

   iii. The private sector should be encouraged to not design devices for 'data exploitation', leaving individuals in control of how their data is used.

   iv. Stakeholders should better understand the security issues and challenges of the Internet of Things (IoT). The technical community and private sector should invest in the development of appropriate security controls for IoT devices.

   v. Culprits of invalid use of information should be charged in line with governing law and breach victims should be compensated per law.

   vi. Ethics standards should be encouraged, and ethics audits of organizations should be encouraged to ensure data is appropriately used within the terms defined by the data holder.

i. **Deploy Secure Development Processes**

   i. A Secure Development Lifecycle should be implemented in all software and product development. The technical community is well placed to develop and release guidance on secure development processes, and share information on ongoing failures to drive process improvement

   ii. Key industry players should raise awareness, and could amongst other sponsor national initiatives for standards.

iii. Stakeholders should identify good standards and protocols, per country, per region, globally (for issues of cultural sensitivity), including protocols for human-computer interaction, and share these widely.

j. **Prevent unauthorized access to devices**

   i. Unauthorized access to devices should be criminalized by enacting appropriate laws. The Budapest Convention offers States a legal framework for prosecuting and dissuading.

   ii. People in developing countries should be better informed about the risks of unauthorized access.

   iii. Policy makers and regulators should encourage, e.g. with economic incentives, IoT vendors to make devices more secure.

   iv. Security and privacy are fundamental rights. Legal frameworks should be in place to allow abuse to be challenged.

   v. Current frameworks lack sufficient safeguards, in law or practice, to address the impact of IoT on human rights. Central elements to a solution are: (1) data protection, (2) best available security practices, (3) transparent international processes on coordinated vulnerability disclosure, (4) the implementation (and, when appropriate, enforcement) of existing standards and or (consumer) laws.

   vi. Citizens should have complaint mechanisms on unauthorized access to or disclosure of sensitive information. Dedicated trained police officers that understand the nature and implications of the issue would allow for a better filing of complaints.

2.1.4. Additional concerns and challenges

In addition to the cybersecurity challenges related to the CENB policy options, and based on the received contributions and BPF discussions, the BPF identified a number of additional cybersecurity concerns that could impact the potential contribution of ICTs and Internet technologies to achieving the SDGs.

a. Mitigate a current lack of cybersecurity awareness through awareness building and capacity development

   i. States should become aware of security risks to their and their citizen's activities. Awareness could be raised by developing best practices and guidelines and sharing them among entities.

   ii. Focus should be put on user education.

   iii. States could contribute to the the general of cybersecurity by encouraging academia to play a bigger role in creating better professionals. Many enterprises are building a workforce that is not experienced in developing secure software. Enabling all ICT professionals to have a strong understanding of security challenges, and of basic software security and network hygiene would solve many cybersecurity challenges long term.

b. Policy and processes should be developed to improve the cyber resiliency of cities.
c. The involvement of women in cybersecurity should be increased.
    i. Diversity in the cybersecurity workforce should be promoted.
    ii. The Internet governance forum and other policy forums should provide mechanisms to ensure women's participation in policy discussions and decision-making.
d. Barriers, such as sanctions on participation in the defensive cybersecurity community, may hamper the ability of organizations to defend themselves effectively from cyber attacks, impacting the security of other networks, including those abroad. Examples include the inability to participate in international conferences, or inability to receive support from equipment manufacturers.
e. Cryptocurrency
    i. Laws should account for the existence of cryptocurrencies and their use in cybercrime, such as acts of ransom, which can be less traceable.
f. Stakeholders should invest in studying the security implications and influence of social media on cybersecurity
g. Whistleblower legislation should be developed and implementated, and administered with excellent judgement.

2.2. Defining responsibilities for the stakeholder communities

After its analysis of the cybersecurity risks and challenges originating from the CENB work, and collecting policy options to address and mitigate them, the BPF discussed responsibilities of the different stakeholder groups and looked for opportunities for further stakeholders cooperation.

Substantial input for this section was generated from the feedback on the call for contributions, and in particular from the responses to the question *'Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?'*

2.2.1. Multistakeholder cooperation on cybersecurity - a shared responsibility

'All stakeholders have a positive role to play in nurturing a trusted and open Internet. We need to work to secure core aspects of Internet infrastructure, to protect the confidentiality and integrity of data that flows over it, and to ensure the right policies are in place to support the technologies, networks and actors that make the Internet work. We do this through collective responsibility and collaboration.'[38]

Each stakeholder community has a responsibility in helping to ensure that cybersecurity does not hinder future Internet development. New technologies may be insufficiently secure and cause harm when deployed, while stringent security requirements may prevent the

[38] BPF contribution the Internet Society

development, deployment, or widespread use of technologies that would generate unforeseen benefits. Stakeholders have the responsibility to foster open inter-stakeholder collaboration and trust relationships, and to infuse a culture of cybersecurity among all stakeholder groups.[39]

Complexity is the reason why multistakeholder efforts are important.[40] There is no one-size fits all solution, and pro-Internet policies can take many different shapes.[41] A multi-stakeholder approach to develop future policies on the strengthening of the rule of law in cyberspace, should involve the relevant stakeholders, so that future policies will represent commonly accepted solutions to make the cyberspace more secure.[42] To succeed, it may be necessary to develop strategies to actively reach out to stakeholders and involve them in discussions on common issues.[43]

From the way the Internet was constituted and works, it follows that 'each party needs to take a collaborative security approach to foster confidence and protect opportunities. Since every stakeholder has different incentives, different economic interests, and different logics (e.g. regarding security/privacy/DP), only a good multistakeholder process would bridge these differences.'[44] Cybersecurity is a collective responsibility, and a culture of cybersecurity should be encouraged.[45] 'Cybersecurity should be considered a 'public good', which promotes collective responsibility for shared benefit.'[46]

On the topic of multistakeholder cooperation on cybersecurity the Internet Society published *Principles of collaborative security*[47] and the *Policy framework for an open and trusted Internet*[48], and the Commonwealth Telecommunications Organisation (CTO) developed the *Commonwealth cybergovernance model*[49].

2.2.3. Stakeholder communities and their responsibilities

<u>Disclaimer - recognising responsibilities is not advocating siloed actions</u>

Cyber issues have become increasingly complex and impact across society and economy. This reality will only aggravate, amongst other with the further development of IoT, making siloed responses an increasingly inadequate answer to mediate cybersecurity issues. Only

[39] BPF contribution Caribbean IGF
[40] BPF contribution Microsoft
[41] BPF contribution the Internet Society
[42] BPF contribution Council of Europe - Cybercrime Division
[43] Contribution Wout de Natris
[44] BPF contribution EuroDIG
[45] BPF contribution Commonwealth Telecommunications Organisation (CTO)
[46] BPF contribution Privacy International
[47] '*Collaborative Security: An approach to tackling Internet Security issues'*, the Internet Society, April 2015, https://www.internetsociety.org/collaborativesecurity
[48] *'A policy framework for an open and trusted Internet'*, the Internet Society, June 2016, https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/
[49] '*Commonwealth Cybergovernance Model'*, March 2014, http://www.cto.int/media/pr-re/Commonwealth%20Cybergovernance%20Model.pdf

reinforced cross-stakeholder group cooperation and multistakeholder approaches will be able to confront and withstand future challenges.

Against this background, it is important that stakeholders are aware of their cybersecurity and cyber hygiene responsibilities, assume them correctly, and have a good understanding of the responsibilities that arise from the activities and competences of the other stakeholder groups. Such an insight will be helpful to identify opportunities for multistakeholder cooperation and joint action, and avoid that initiatives by different stakeholders work counterproductive and fail to contribute to an increase of the overall level of security.

The BPF Cybersecurity called upon the community to help identify the responsibilities of the different stakeholder groups. Substantial input for this section was generated from the responses to the question *'Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?'*.

Governments (and International organisations)

There's an opportunity for governments to take 'a leading role in driving a national and international cybersecurity agenda and setting regulatory and policy priorities'.[50] 'They play a fundamental role in developing policy and legal frameworks for a secure cyberspace, data protection, protecting critical information infrastructure and enforcing the law against cybercrime, online abuse and gender based violence.'[51] Governments play an essential role in protecting critical infrastructure and prosecuting cybercriminals,[52] and should support and cooperate with banks, credit card companies, insurance companies, cell phone companies, and other businesses vulnerable to fraud. Governments can facilitate, initiate and/or (financially) support processes that lead to a better cybersecurity environment, e.g. through initiating (discussions on) ISACs, anti-abuse mechanisms, anti-DDoS facilities, etc., and encourage industry to take the lead.

Nations should seriously consider putting in place a robust risk management system, driven by a common cybersecurity strategy. A countrywide vulnerability management strategy is indispensable. Policies should be in place to ensure stakeholder transparency and accountability in ISP, DNS and IXP communities.[53] Governments could take initiatives for business, SMEs and entrepreneurs to inform about cybersecurity risks, and support by sharing advise and best practice examples.[54]

[50] BPF contribution EuroDIG
[51] BPF contribution Luisa Lobato
[52] BPF contribution Microsoft, BPF contribution IGF Mauritius
[53] BPF contribution Opeyemi Onifade
[54] For example the announced Dutch Digital Trust Centre, https://www.rijksoverheid.nl/actueel/nieuws/2017/09/23/digital-trust-centre-geeft-ondernemers-advies-over-cybersecurity (webpage in Dutch)

In terms of policy, governments could encourage solid technology practices such as bug bounties[55], and not exacerbate the problem by hoarding vulnerabilities or by creating backdoors in secure communications technologies. Governments have the ability to regulate private sector through data protection laws and other consumer protection measures. They should pursue policies or treaty options that compel signatories to abide by international principles, norms and standards that ensure that cybersecurity and national security measures that employ digital technology are necessary and proportionate. Governments and private sector should cooperate in private sector-government partnerships to improve transparency and to protect disclosures.[56]

The fact that in many countries, different government branches are responsible for ICTs, intelligence, national security, and sustainable development poses an extra challenge.[57] When taking on their role, governments should be cautious not to 'undermine the collaborative approaches and the role of the technical community and industry in identifying risks, providing security of networks and customers, and the role of civil society in safeguarding transparency, accountability, due process and human rights. They should not 'fuel competition for creating insecurity (...) and not undermine user's data protection,'[58] for example by stimulating offensive security research to expose vulnerabilities without an intent to fix.

Modern methods of attack may require tackling of cybercrime internationally through aligning legislative initiatives,[59] and International organisations should ensure 'that all governments do adopt conventions and agreements'[60] at the same time and at the same level.

Governments have the responsibility to reach out and engage with other stakeholders in seeking multistakeholder solutions to cybersecurity challenges as noted and recommended in the prior section on multistakeholder approaches.

There is much potential for a more global conversation and bottom-up discussions about interoperability of legal regimes that apply to this area, amongst other on common understandings of the privacy-cybersecurity discussion, on how information sharing can be designed to have minimal impacts on privacy and competition, on developing cybersecurity regulation without stifling innovation, and on other areas where the public-private interface could be developed, and have a global application. The IGF, as a pluralistic and multifaceted platform could facilitate such discussions.[61]

[55] See for example the 2015 BPF on Spam on 'Responsible Disclosure'.
[56] BPF contribution Association for Progressive Communications (APC)
[57] BPF contribution Association for Progressive Communications (APC)
[58] BPF contribution Luisa Lobato
[59] BPF contribution Microsoft
[60] BPF contribution IGF Mauritius
[61] Paraphrasing Amit Ashkenazi, Israel National Cyber Directorate, at the Cybersecurity coordination session, Geneva, 21 December 2017.

Civil Society

While governments usually take the lead in setting policy and regulatory priorities, the role of civil society is important in monitoring accountability and transparency, and safeguarding due process and human rights.[62]

NGOs have a critical role in raising awareness, and promoting responsible behaviour and safety online.[63] Their activities are fundamental for pressing governments to abide by their obligations to respect rights such as privacy and freedom of expression, for increasing awareness over rights in the digital age, for promoting responsible behavior, and for spreading best practices.[64] NGOs have been important hubs for expanding access policies in developing countries, often being closer than other actors to the everyday challenges faced by users.[65]

Technical community

It is the responsibility of the technical community and industry to identify risks, provide security of networks, devices and people.[66]

It is important to support efforts to mitigate DDoS and other attacks at the technology level, rather than with policy such as criminalisation. Proactive solutions to find, mitigate and disclose vulnerabilities are key to addressing reliability and access. The technical community must develop protocols to prevent their use for exploits such as DDoS.[67]

Technical organisations, such as the IETF, could consider broadening their membership to include all stakeholders, and involve NGOs and stakeholders in their discussions before designing the technical solutions.[68]

Multistakeholder cooperation within the IETF and other standardising bodies could on the one hand focus on the swift implementation of standards developed by and with the technical community to ensure a safer environment, while on the other hand, concentrate on identifying urgent issues together.

Private sector

The private sector should adopt the principle that the best security is the one that is not noticed by the secured. The private sector plays a core role in developing secure technology,

[62] BPF contribution EuroDIG
[63] BPF contribution Microsoft
[64] BPF contribution Luisa Lobato
[65] BPF contribution Luisa Lobato
[66] BPF contribution EuroDIG
[67] BPF contribution Association for Progressive Communications (APC)
[68] BPF contribution IGF Mauritius

secure products and services, as well as in sharing knowledge and best practices[69] with governments and non-governmental organizations.[70]

The private sector must use due diligence to protect human rights, and avoid adverse impact. They have to ensure the correct implementation of protocols and best practices. They must create readable ToS for users, and proactively inform users of software updates.[71] In addition, it must evaluate its approach from the users' perspective, taking into account user groups with special needs, e.g. elderly or disabled people, for who information and awareness alone might not be effective.[72] Consumers should be made aware of their responsibility in terms of cyber hygiene and of the technical security possibilities of the devices they use to connect to the Internet, to better enable them to help to protect their own security and the network itself.[73]

Academia

The Academics' main responsibility is to guide with scientific research.[74] To avoid a knowledge gap, it is important that also the most recently developed and adopted technologies are included in academic curriculums and research programmes.[75] Academic institutions should contribute to a better education and training of professionals with the right competencies and mindset.[76] Academics and security experts should monitor[77] best practices implementation.[78] Policy protections should exist for researchers that seek out vulnerabilities in technology in the public interest.

Section 3: Areas to develop further stakeholder conversation

The 2017 BPF Cybersecurity was inevitably limited in time and scope, but looked beyond these limitations by exploring and identifying areas and issues that would benefit from further multistakeholder approach. Many issues are already being discussed and dealt with by one or more stakeholder groups in specific forums. Where this is the case, one should avoid duplicating by creating a new forum or platform, but instead look for opportunities to establish dialogue and cooperation between existing initiatives. Likewise, interested

[69] For example, '*Duties of Care in ICTs'*, published by the Dutch Cyber Security Council, https://www.cybersecurityraad.nl/binaries/20170518_DEF%20CSR_HandreikingZorgplichten_EN_web_tcm56-260893.pdf
[70] BPF contribution Microsoft, Luisa Lobato
[71] BPF contribution Association for Progressive Communications (APC)
[72] BPF contribution Delfi Raminez
[73] Paraphrasing Matthew Shears, GP Digital, at the BPF Cybersecurity workshop, Geneva, 20 Dec 2017.
[74] BPF contribution China
[75] BPF contribution IGF Mauritius
[76] Paraphrasing Cristine Hoepers, CERT.br, at the BPF Cybersecurity workshop, Geneva, 20 Dec 2017.
[77] For example the work of Michel van Eeten e.a., Technical University Delft, on the measurement of effectiveness of implementing best practices and cybersecurity measures.
[78] BPF contribution Association for Progressive Communications (APC)

stakeholders are advised to consider joining the existing forums and help to further develop the multistakeholder dialogue on the issue at stake.

Substantial input for this section was generated from the contributions, and in particular from the responses to the question *''What is the most critical cybersecurity issue that needs solving and would benefit from a multistakeholder approach?'* and further BPF discussions.
The existing forums mentioned below should be considered as a non-exhaustive list of examples.

Areas to develop further stakeholder conversation

1. Fostering a **culture of cybersecurity**, and making sure it is accessible and understood by each stakeholder group; and developing a better **set of core values around cybersecurity**. Ensure full representation and participation of developing countries in the IGF process.
   Existing forums: UNIDIR.[79]

2. Development of internationally-agreed **cybersecurity norms.**
   Existing forums: UNGGE, GCSC.

3. **Internet of Things ecosystem security**, which accounts for the convergence of safety and security principles and the lack of commercial incentives to secure these devices and services it.
   Existing forums:
   - US Internet of Things Cybersecurity Improvement Act of 2017 (https://www.congress.gov/bill/115th-congress/senate-bill/1691)
   - IoT Alliance Australia (http://www.iot.org.au/)
   - Cloud Security Alliance IoT Working Group (https://cloudsecurityalliance.org/group/internet-of-things/#_overview)
   - IoT Security Foundation working groups (https://www.iotsecurityfoundation.org/working-groups/)
   - Online Trust Alliance IoT vision (https://otalliance.org/initiatives/internet-things)
   - Open Group Internet of Things Work Group (https://otalliance.org/initiatives/internet-things)
   - US NTIA Internet of Things Call for Input (https://www.ntia.doc.gov/category/internet-things)
   - Europol-ENISA IoT Security Conference (https://www.europol.europa.eu/events/europol-enisa-iot-security-conference)

[79] *'The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century'*, UNIDIR, 2017, http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

- Trusted Computing Group IoT work group (https://trustedcomputinggroup.org/work-groups/internet-of-things/)
- Internet2 CINO Working Group on the Internet of Things (https://spaces.internet2.edu/pages/viewpage.action?pageId=88573855)
- RIPE IoT Working Group (https://www.ripe.net/participate/mail/ripe-mailing-lists/iot-wg)
- NIST Cybersecurity IoT program (https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program)
- IGF Dynamic Coalition on IoT (http://www.intgovforum.org/cms/component/content/article/118-dynamic-coalition-proposals/1217-dynamic-coalition-on-the-internet-of-things)
- Petras IOT hub (https://www.petrashub.org/)

4. Vulnerability of **critical infrastructure and Internet resources.**

   Existing forums: Meridian, GFCE, ISACs.

5. Ensure that risk management approaches **acknowledge that security is an evolutionary process**, and that no security deployment can offer 100% protection.

   Existing forums:

6. **DoS/DDoS attack, BGP/IP prefix hijacking and DNS abuse.**

   Existing forums: NANOG, FIRST, RIPE, APNIC, AFRINIC, LACNIC, NAWAS of the NBIP.

7. **Cybercrime.**

   Existing forums: Europol, Interpol, UNODC, Council of Europe.

8. **State stability and peace in cyberspace.**

   Existing forums: OSCE, UN.

9. **Ransomware.**

   Existing forums: No More Ransom.

10. Lack of **education** and end user awareness/engagement.

    Existing forums:

11. **A Framework to foster international cooperation and legal principles** for cybersecurity could be developed in the UN framework.

    Existing forums: GCCS, Council of Europe.

12. Cognitive computing and **Artificial Intelligence.**

    Existing forums:

13. For **mobile networks**: (1) lack of public and available professional forums to address security threats, (2) low awareness of system administrators in securing next generation networks, (3) expansion of the Internet of Things.

    Existing forums: GSMA.

14. A stronger reflection of **criminal justice aspects** is needed in cybersecurity policies.

    Existing forums: Eurojust.

15. **Extreme threats:** Security threats in the digital world evolve faster than established rules, laws and even technical knowledge (i.e. in case of ransomware or other threats of the nascent IoT).

    Existing forums:

16. **Asymmetric use and access** to the Internet.

    Do cyber threats of different natures pose a greater threat to open societies than to closed ones? From organised crime to democracy undermining activities. Do governments undertake enough or the right activities to protect their respective citizens, institutions and companies?

    Existing Forums:

17. **Anti-abuse initiatives.**

    Around the world there are organisations fighting abuse through the setting of Internet standards or direct actions against the use of abuse sources.

    Existing Forums: M3AAWG, AbuseHUB, Signal Spam, APWG, Stop Think Connect.

Part III: Conclusions and way forward

The 2017 Best Practice Forum on Cybersecurity examined how a well-developed cybersecurity helps to create an enabling environment for ICTs and Internet technologies to contribute to development, and to help achieve the UN Sustainable Development Goals (SDGs). Poor cybersecurity risks reducing the effectiveness of ICTs and Internet technologies, and thus limits their ability to help achieve the SDGs.

The BPF analysed the IGF's Policy Options for Connecting and Enabling the Next Billion(s) (CENB) for cybersecurity challenges and compiled, based on community input, sets of policy suggestions to mitigate these risks. These suggestions are intended to inspire policy decision makers around the world. An analysis of stakeholder roles and responsibilities learned that each stakeholder group can contribute to a better cybersecurity, by own actions and initiatives, and by participating in the exchanges and dialogue with other stakeholders. Therefore the BPF identified cybersecurity issues that could benefit from further stakeholder dialogue.

The BPF Cybersecurity was conceived as a multiyear project that grew out of previous BPFs on CSIRTs and on Spam mitigation. In 2016 the BPF Cybersecurity studied how enhanced collaboration and collaboration between stakeholders can contribute to building confidence and security in the use ICTs. In 2017, as mentioned, the BPF focussed on cybersecurity and development. At the IGF meeting in Geneva the BPF started an exchange to explore possible ways forward and potential topics for a continuation of the BPF Cybersecurity in 2018 and beyond, should the MAG decide to retain cybersecurity as a topic for a BPF.

Possible future development for the BPF Cybersecurity

The BPF Workshop in Geneva zoomed in on two of the areas that, according to the public contributions to the BPF, would benefit from further stakeholder conversation (see Section 3), and hand an exchange of views on '*Defining and identifying a cybersecurity culture, norms and values,'* and '*Identifying the risk of a potential digital security divide, between those who have and those who do not have access to cybersecurity measures'* as possible topics for a BPF on cybersecurity in 2018, if organised. (see the Workshop report for more details).

An informal BPF Cybersecurity Coordination session, open to all interested, convened on the last day of the IGF meeting in Geneva, to discuss the work of the BPF in general, rather than the subject matter which was addressed during the BPF Workshop, and to have an exchange of ideas on where to take the BPF in future years, if renewed.

The session reflected on how the BPF contributed to the wider IGF goals by creating a multistakeholder space to collect best practices and experiences around cybersecurity from a wide variety of stakeholders, including by leveraging the National and Regional IGF communities. These discussions and exchanges at IGF level, it was said, help to build more common understanding between all parties involved, provide an opportunity to exchange views on areas where no consensus exists, and create a space for learning about topics that are not yet at a level of shared understanding.

Government representatives participating to this coordination session noted that in order to improve government participation in it's work, the BPF would benefit from collecting best practices which everyone should apply, but which may not (yet) be universally known or shared. While it was understood that cybersecurity included sensitive issues governments would not be ready to address in an open setting, government participants recognised the necessity to engage with non-governmental stakeholders.

The full report on the BPF coordination session can be found in the annexes.

Annexes

Annex 1: contributions to the 2017 BPF Cybersecurity

The BPF on Cybersecurity received 27 formal contributions in reaction to its August 2017 public call for contributions. The contributions are archived on the IGF website[80]. The BPF wishes to thank all contributors for their valuable insights and ideas.

-Mr. Shredeep Rayamajhi

-Mr. Ben Wallis / Microsoft

-Dr.N.Sudha Bhuvaneswari

-Mr. Foncham Denis Doh / Cameroon Internet Governance Organization

-Mr. Ji Haojun / Government of China

-United Nations Cuban Association

-Ms. Anita Sohan / Commonwealth Telecommunications Organisation (CTO)

-Mr. Mohit Saraswat

-Mr. Akinremi Peter Taiwo / African Civil Society on Information Society (ACSIS)

-Mr. Peter Micek / Access Now

-Mr. Naveen K. Lakshman

-Ms. Carina Birarda / ISOC Cybersecurity SIG

-Ms. Luisa Lobato

-Mr. Dave Kissoondoyal / IGF Mauritius

-Dr. U.M. Mbanaso / Centre for Cyberspace Studies, Nasarawa State University

-Ms. Amali De Silva-Mitchell

-Mr. Opeyemi Onifade / Africa ICT Alliance (AfICTA)

-Mr. Mohammad Talebi / Mobile communication Company of Iran (MCI)

-Ms. Lucy Purdon / Privacy International

-Mr. Koen van den Dool / Global Commission on the Stability of Cyberspace

-Mr. Alexandru Frunza-Nicolescu / Cybercrime Division, Council of Europe

-Mr. Sivasubramanian Muthusamy / Internet Society India, Chennai Chapter

[80] https://www.intgovforum.org/multilingual/content/bpf-on-cybersecurity-contributions

-Ms. Raquel Gatto / ISOC [Additional Report]

-Mr. Nigel Cassimire / Caribbean IGF

-Mr. Arzak Khan / Internet Policy Observatory Pakistan

-Ms. Mallory Knodel / Association for Progressive Communications (APC)

-Ms. Tatiana Tropina / EuroDIG

Annex 2: CENB Phase I & II Cybersecurity-focused policy analysis

CENB Phase II - Cybersecurity-focused policy analysis

Analysis contributed by Andrew Cormack

Notes on how cyber-security can affect the achievement of the Sustainable Development Goals (SDGs). Derived from the IGG Policy Options for Connecting and Enabling the Next Billion(s): Phase II. Many of the cyber-security issues affect several SDGs: the connections selected here are chosen as perhaps the best examples of these dependencies.

SDG1 (No Poverty) depends on individuals being able to access information over the Internet. Thus it can be disrupted by weaknesses in, and attacks on, the availability of information services and the networks that individuals use in connecting to them. Issues such as **denial of service attacks** and **services that can act as amplifiers** for them could therefore affect progress towards this goal. Similar issues arise in SDGs 4 (Quality Education), 10 (Reduced Inequalities), 14 (Life below water) & 15 (Life on Land), and the overall aim of providing “meaningful access”.

SDG2 (Zero Hunger) includes farmers seeking information, reporting on local conditions, applying for grants etc. Since such activities may involve implicit or explicit criticism of public authorities, they will be hindered by any perception that those authorities are engaged in **surveillance of Internet usage**.

SDG3 (Good Health) includes telemedicine, disease monitoring and the storage of patient data. Developed countries have already experienced setbacks in these areas as a result of incidents affecting the **confidentiality and availability of sensitive information** held by medical and health services.

SDG5 (Gender Equality) is harmed by individuals or organisations using communications technologies to engage in **online abuse** and gender-based violence.

SDG6 (Clean Water) involves using communications technologies for the remote monitoring and control of treatment and pumping equipment. **Vulnerabilities in SCADA (Supervisory Control and Data Acquisition) equipment** that is connected to shared networks are a major concern that can turn such automation from a benefit into a serious pollution and health threat.

SDG7 (Affordable and Clean Energy) depends on the widespread acceptance of smart meters and smart grids. Loss of trust in these systems can easily be caused if monitoring equipment and systems do not keep information confidential, or if **information is used for inappropriate purposes**.

SDG8 (Decent Work and Economic Growth) highlights the importance of mobile payment systems, which are critically dependent on the **security of mobile devices** such as phones and tablets.

SDG9 (Industry, Innovation and Infrastructure) suggests that developing countries may find opportunities to develop disruptive industries in the area of IoT (Internet of Things). However **lack of secure development processes** are already causing concerns for IoT and any industry based on them could be severely damaged by a security failure in its products.

SDG11 (Sustainable Cities and Communities). Many of the technical tools suggested as supporting this aim can also become serious threats to individuals and communities if they are not secure. Criminals, neighbours, governments or even family members with **unauthorised access** to Internet-monitored home security, traffic monitoring or CCTV systems can cause serious privacy, material, physical or emotional harm.

SDG16 (Peace and Justice) concerns citizen engagement in government, but also notes that these tools can be used for repression and the spread of prejudice. Either will strongly discourage engagement. Systems used to hold authorities to account must be **protected from abuse by those authorities**.

CENB Phase I - Cybersecurity-focused policy analysis

Analysis contributed by Maarten Van Horenbeeck

The 2017 Best Practices Forum on Cybersecurity is reviewing the cybersecurity implications of policy recommendations made as part of "*Policy Options for Connecting and Enabling the Next Billion(s): Phase II*". The outcome of this work will help inform policy makers of the important cybersecurity implications of implementing or evaluating a specific policy option.

In order to ensure a comprehensive review, these notes describe a review of the cybersecurity implications of policy options identified as part of "Policy Options for Connecting and Enabling the Next Billion(s): Phase I". While that document did not align with the Sustainable Development Goals, and thus will not be our line of inquiry in approaching the Phase II review, this review is intended to ensure our guidance is comprehensive.

In Appendix A, a set of reviewed policy recommendations, extracted from the Phase I CENB document is listed. Reviewing those, I identified a set of high-level criteria which came up, in many cases repeatedly. I noted some brief security implications of each:

1. Promoting improved and extended broadband infrastructure:
   - Increased broadband increases the risk of vulnerable endpoints being leveraged in high-bandwidth **Distributed Denial of Service attacks**. Whereas unmaintained, unpatched or unlicensed devices on low bandwidth networks have mostly localized impact, on high bandwidth networks the impact is likely to have more implications at the global network level.
2. Promoting spectrum increases and promoting increased reliance on wireless modes of operation:
   - Use of spectrum for Internet access is subjected to **local jamming as a Denial of Service attack**, which has different recovery scenarios (they must be triangulated and stopped) than cable disruptions (which can physically be fixed).
   - Wireless network access increases the importance of **strong traffic encryption** controls.
3. Promoting increased power grid capacity:
   - Extension of power grid capacity, in particular over greater distances will involve the deployment and reliance on the **security of Supervisory Control and Data Acquisition (SCADA) equipment**.
4. Promoting the development of Internet Exchange Points:
   - Internet Exchange Points have strong physical security needs, and imply the use of specialized software and hardware which must be maintained. Use of components with **good software security and a standard, maintainable and updatable setup** becomes more important as IXPs are more distributed and perhaps run by local teams with less experience.
5. Promoting user awareness education:

- Educating users on the use of the Internet requires those users to be **made aware of security risks and safe conduct online**.
- It requires the **development of initial services with human behavior in mind**, so the default behavior of users on the services they use as their first entry online is secure.

6. Deploying government services using an Open Data model:
   - **Making data available requires proper anonymization**, which is not an easy challenge. Data must be available in aggregate to be of use, but should not be released in such way that permits de-anonymization.
   - Data released by the government must have **strong integrity** to enable society to make appropriate decisions based on its analysis.
   - When third parties start building on top of the data set, its **availability** becomes important to permit these third parties to function.
7. Addressing unsolicited e-mail and other forms of spam:
   - Spam and unsolicited messages may make otherwise effective communication channels difficult or unpleasant to use. **Abuse management mechanisms** are needed, which should be carefully introduced so as not to lead to censorship or put in place other boundaries on communication.
8. Promoting the increase of locally relevant content and local language support:
   - Increased local language support, in particular when associated with other character sets may increase the risk of **homoglyph attacks** on the URIs used for such content, or other, international content;
   - Locally relevant content may not be required to be available globally. These reduced performance requirements may incentivize content creators to store it on local network resources. Having only a single copy of the information available in a region increases the risk of a **Denial of Service attack** rendering it unavailable, or a local outage causing it to be destroyed.
9. Promoting national domain name infrastructure:
   - National domain name infrastructure is often less robust than the gTLD's on which large international enterprises are deployed, such as .com, .net and .org. Increasing reliance on it requires investment in **secure domain name and registry infrastructure**.
10. Promoting sharing of passive infrastructure:
    - Shared infrastructure may expose infrastructure owned by one operator to another, requiring the implementation of **strong security controls** restricting access;
    - Shared infrastructure **reduces overall redundancy of networks**. An outage of a single site may affect multiple providers.
11. Addressing minority and gender-based online harassment:
    - Addressing minority or gender-specific harassment requires contextual knowledge of what "harassment" means and proper reporting channels. These reporting channels may not always be available when a service provider is in a different country, or operating under a different legal framework.
12. Strengthen telecommunications infrastructure through public private partnerships:
    - Public-private partnerships may include shared operational capability between government and industry providers, which requires **strong security controls and separation of duties** to ensure the public partners are unable to affect technical implementations e.g. domestic surveillance.
13. Enabling initiating economic opportunities, such as starting a company online:
    - Bringing services critical to the economy online requires secure development processes to ensure the **underlying data stores are protected from unauthorized access and modification**;
    - A **Denial of Service attack** against such services may hamper the ability of businesses to do their work, or citizens to become economically active.
14. Make Internet devices more affordable
    - Increased price pressure without specific quality requirements may result in vendors saving on costly, but important processes such as **quality control**. This may result in devices being introduced without passing through a software development lifecycle that includes security testing, or a supportable update process.

Appendix A: Policy options identified from the Phase I document

http://www.intgovforum.org/cms/documents/policy-options/654-igf-policy-options-for-connecting-the-next-billion-compilation/file

1. Deploying infrastructure

a. Physical, interconnection layers and enabling technologies

- *I.* Promote broadband infrastructure (Africa IGF)
- *II.* Promote power grid capacity (Africa IGF)
- *III.* Explore creation of continental common toll-free Internet platform to preserve the identity and cultural heritage of Africa (Africa IGF)
- *IV.* Stabilize pricing for Internet access service (Ministry of Comm. Brazil)
- *V.* Improve transcontinental submarine cabling (Ministry of Comm. Brazil)
- *VI.* Groups with major market power are obliged to connect to traffic exchanges, offer full peering, paid peering and traffic (Ministry of Comm. Brazil)
- *VII.* Stimulate investments for broadband roll-out (EuroDig)
- *VIII.* Provide public funds where private investment is not enough (EuroDig)
- *IX.* Development of public-private partnerships (EuroDig)
- *X.* Open access and spectrum for Wi-Fi development (APrIGF)
- *XI.* Spectrum is a common good, policy should be inspired by criteria of public and general interest (EBU)
- *XII.* Pro-competitive broadband policy (ICC Basis)
- *XIII.* Policy initiative targeted at specific socio-demographic groups (Annenberg School for Communication)

b. Mobile

- I. Half of the world's population has a mobile subscription – mobile helps to provide underserved regions with the opportunity to overcome socio-economic challenges (GSMA)
- II. Making prepaid mobile services available to non-elites, increasing mobile competition to reduce prices (ICT Africa)
- III. Stimulate 3G networks in Niger – mobile credited for nearly all progress on connectivity (IGF Niger)
- IV. Promote wireless in areas with reduced electricity coverage (Movimento de Espectro Livre)
- V. Spectrum is finite, ITU estimates 1340-1960 Mhz of spectrum required for 2020 demand (GSMA)

c. Funding sources: Universal service funds, Public Private partnerships

- I. Universal Service Provision Funds should be used to engender infrastructure into underserved areas and enable affordability (African Regional IGF)
- II. USAF should address institutional environment: oper. Independence, legal clarity, internal capacity + support broadband supply. Successful funds are targeted to address affordability and gaps (Alliance for Affordable Internet)
- III. Investments are currently typically redirected to urban and semi-urban areas (Universal Access Fund and ICT Infrastructure Investment Africa)

d. Deployment

- I. Development of IXPs and IPv6/IDN deployment play a crucial role (EuroDig)

2. Increasing usability

a. Applications

I. Causal relationship between low usage of mobile media tools and Internet literacy – even when people have access to the Internet, they lack the understanding of it (World Bank)

b. *Services*

I. Citizens need to have information on what governments and private sector are doing to increase access and connectivity, especially in rural areas. Geography and culture must be taken into account (civil society)

II. Digital content and services are important to drive Internet adoption and usage (World Economic Forum)

c. *Local Content, Multilingualism*

I. Content in local languages is important – accessible, cheap and interesting are content requirements (EuroDig)

II. Representation and participation are uneven, many people are left out of the debate (IGF local content 2014)

III. Encourage locally relevant content, including protections for freedom of expression, press, privacy and intellectual property, e-commerce infrastructure, consumer protection, trusted online payment systems. Policies must be market driven and based on voluntary commercial arrangements (ICC Basis)

IV. Promote local content (Iberoamerican federation of IT associations)

V. Local content promotion in Spanish and native American languages (Paraguay IGF)

d. *Media*

I. Most traffic is driven by professionally produced quality content. Local content promoters are now in competition with global content industry (EBU)

e. *Accessibility*

I. Legislative framework on accessibility exists, but awareness raising, education and training of specialists is needed. (Swiss IGF)

II. Items paid for by the public must be accessible for the public – open access to publicly funded research (Swiss IGF)

3. Enabling users

a. *Human Rights*

I. States and private sector must commit to developing clear standards, procedures for protection and transparency to strengthen human rights on the Internet in the region (Asia Pacific Regional IGF)

II. African IGF session on Human Rights on the Internet:
1. Establish mechanisms to promote, monitor and popularize African Declaration on Internet Rights and Freedoms and UNESCO's concept of Internet universality
2. Self regulatory, independent objective oversight and sanctioning mechanisms
3. Meaningful access to ICT includes control over ICTs as a key resource towards advancing status of women and girls and their human rights
4. Address emerging issue of violence against women

b. *Inclusiveness (Gender, Youth)*

I. Issues: unequal access to Internet infrastructure, affordability, gender disparity in education, digital literacy, uneven capacity to use Internet for needs and priorities, specific gender-based challenges and barriers (relevant content, gender-based harassment and violence) (2015 IGF BPF on Countering Abuse against Women online)

c. *User literacy*

I. Support open data models, local content development, eLearning initiatives (African Regional IGF)

II. Principles on Public Access in Libraries (IGF DCPAL) *d.* *Digital Citizenship*

I. Fostering public access points in public libraries and community centers, and promoting content creation and digital literacy activities in those places (LAC IGF)

II. Accessible voting machines, supporting school for blind students, working with low income populations. Promoting access to information. (Microsoft)

e. *Entrepreneurship*

I. Those formerly excluded from economic opportunity can use the Internet for all phases of starting their own companies (WEF 2015)

4. Ensuring affordability

a. *Digital divide*

I. Improve investment in R&D to allow Brazil to compete with foreign-produced goods. Otherwise the country does not fully benefit from the Internet economy (Movimento de Espectro Livre – Brazil)

II. Focus on increasing supply and lowering cost of access (Internet Society)

III. Address spectrum availability for 3G and 4G (Arab IGF)

IV. Increase IXPs at national and regional levels (Arab IGF)

V. Educate on computer literacy and reduce device cost, which will drive Internet use and support establishment of local content (Arab IGF)

b. *Costs of Access per Capita*

I. Infrastructure sharing (e.g. independent tower companies) lowers industry costs (Alliance for Affordable Internet)

II. Identify appropriate balance between taxation revenue and long-term socio-economic growth. Develop evidence based policies (Alliance for Affordable Internet)

III. Develop firmware for devices already on the market, so existing devices can be re-used (e.g. OpenWRT) (Movimento de Espectro Livre – Brazil)

5. Creating an enabling environment

a. *Government, Regulatory Authorities and IGO frameworks, laws and regulations*

I. Connecting the next billions should be driven as a project (African Regional IGF)

II. Ministries of Communications should review plans through multistakeholder cooperation (African Regional IGF)

III. Governments should demonstrate ability to implement viable policies already in place (do not replace previous govt projects) (African Regional IGF)

IV. Deploy government services using open data model (African Regional IGF)

V. Effective monitoring of projects and online reporting (African Regional IGF)

VI. Regional multistakeholder approach at the AU-level (African Regional IGF)

VII. Infrastructure sharing at the backbone level and open access to cut costs (Mozambique IGF)

VIII. Fiscal policy and taxation (Mozambique IGF)

IX. Research and Data Collection (Mozambique IGF)

X. National broadband strategies require extensive public consultation with all stakeholder groups (APC)

XI. Eliminate market protections for incumbent operators (APC)

XII. Increase government investment in public access facilities and awareness raising, focused on disenfranchised groups (APC)

XIII. Allow innovative uses of spectrum and new spectrum sharing techniques (APC)

XIV. Promote local ownership of small-scale communications infrastructure (APC)

XV. Using public funds and utility infrastructure to ensure national fibre networks move into sparsely populated areas (APC)

XVI. Adopt effective infrastructure sharing (APC)

XVII. Reduce taxes on ICT goods and services (APC)

XVIII. Established broadband targets in Digital Agenda for Europe (EC)

XIX. Creation of ad-hoc funds to stimulate investment (EC)

XX. Improve digital skills and literacy (Coding week, networks of Digital champions) (EC)

XXI. International organizations should show benefits of investments in access, high capacity connectivity, promote healthy, competitive and stable market environments, develop private-public partnerships for non-commercially viable areas, transfer expertise and share best practices (EC)

XXII. Promote corporate social responsibilities (Nigeria IGF)

XXIII. Broadband policy, ICT Policy encouraging investment and Local Content Policy (Nigeria IGF)

b. *Private sector-led initiatives and market strategies*

I. Alliance for affordable Internet:

1. Liberalized market with open, competitive environment
2. Nurture healthy market competition
3. Streamline licensing process with no barriers to market entry
4. Ensure competitive market structure, with no govt ownership of end user providers
5. Available access at market rates to international gateway or cable
6. Transparent disclosure of pricing and service options
7. Permit pre-paid and tiered pricing
8. Remove barriers to crossing national borders with infrastructure or traffic

II. ICC Basis:

1. Open and competitive markets, fair, investment-friendly, comparable regulatory intervention for all actors
2. Strong reliance on voluntary commercial arrangements
3. Policies that promote efficiency through engineering-driven design (creation of IXPs)
4. Policies that promote growth of products and services provided over broadband

III. Run localized networking initiative with solar backup (Kenya IGF)

IV. Social enterprise that makes broadband available at low cost, based on national fiber optic network (Kenya IGF)

c. *Non-profit, Public-Private partnerships and Other initiatives*

I. Arab IGF:

1. Foster private-public partnerships to invest in telecom infrastructure to reach out to disadvantaged areas
2. Establish national and local dialogues on benefits of Internet and how it improves economic situation of individuals
3. Develop policies and regulations that cater for competitive access-price strategy, macro-level affordability
4. Engage with CSOs to reinforce their role in mobilizing communities they work with

II. Facilitiate deployment of telecoms infrastructure to facilitate access to spectrum and lower taxes (LACIGF)

III. Companies must develop business models to break restriction income. Universalize through mobile telephony (LACIGF)

IV. Digital inclusion programs such as distributing computers to children in schools (LACIGF)

V. Invest in network services in order to close coverage gap (LACIGF)

VI. Roll-out of optic cables throughout country (Benin IGF)

VII. Promote national TLD (Benin IGF)

VIII. Federal Telecommunications Institute of Mexico:

1. Promote access for persons with disabilities
2. Make terminal devices and telecom services more affordable and better quality to ensure widespread access
3. Strengthen telecoms infrastructure by encouraging public-private partnerships
4. Encourage campaigns for skills building
5. Encourage multi-stakeholder governance

IX. Facebook:

1. Reduce the cost of Internet access, such as supporting innovative business arrangements like free basics
2. Promote free and open Internet
    a. Do not permit fast lanes, blocking, throttling
    b. Do not introduce laws inhibiting innovation
    c. Innovative practices such as zero-rating can give more people access to content
3. Expand connectivity infrastructure
    a. Streamline local licensing processes
    b. Reduce legal barriers to entry
    c. Promote sharing of passive infrastructure (dig once, build once)
    d. Tax incentives can accelerate development

X. Colombia IGF:

1. ICT appropriation linked to access is important to increase impact of government initiatives and reducing digital divide
2. Promote production of software and local content with social focus
3. Encourage public Internet access strategies, and do not neglect them in favor of mobile access. Public access links vulnerable communities.
4. Expand community wireless networks and connection of schools and libraries to rural areas
5. Reduce or eliminate taxes related to Internet access and devices
6. Reduce gender gap and ICTs

XI. Broadband commission:

1. Prioritize supply and demand-side policies to full range of broadband infrastructure, applications and services
2. Initiate and prioritize broadband planning process
3. Invest in ICTs and digital skills as engine of growth
4. Review and update regulatory frameworks to take into account evolving models

XII. Expand private and public sector engagement, augment stakeholder community, recruit leaders from various sectors (civil society)

XIII. More regional cooperation initiatives to address lack of domestic political will (IGF Niger)

XIV. Microsoft:

1. Openness to dialogue across partners institutions and organizations
2. Inclusiveness of local actors aware of local needs
3. Enabling environment for joint planning and execution
4. Identification of socio-economic development opportunities and priorities
5. Application of successful models across disciplines

XV. Promote public-private partnerships for connecting remote regions (Telefonica)

XVI. Address unsolicited e-mail

Annex 3: Report of the BPF Cybersecurity session at the 2017 IGF meeting

IGF2017 BPF Cybersecurity
20 December 2017, Geneva, Switzerland
Workshop report

Video https://youtu.be/rXFBpR_2eYA

Background
The Best Practice Forum (BPF) on Cybersecurity is part of the 2017 IGF intersessional work programme and aims to provide a broad multistakeholder platform for engagement on cybersecurity matters. The BPF's output document is part of the tangible outcome of the 2017 IGF.

Introduction

- BPF Co-Facilitator *Markus Kummer* reiterated that the BPF on Cybersecurity was conceived in 2016 as a multi-year project that grew out of and builds upon the work of the BPF on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet security and the BPF on Regulation and Mitigation of Unsolicited Communications, both of which ran during 2014 and 2015.

- BPF Lead-Expert *Maarten Van Horenbeeck* explained that the goal of the Workshop was to have an exchange with experts and the IGF audience on the cybersecurity challenges and policy options identified in the draft BPF output document; to discuss possible valuable areas and work for the BPF in future years; and to launch the discussion on a proposal to continue the BPF on Cybersecurity in 2018 that will be submitted to the IGF MAG for consideration.

- BPF Co-Facilitator and Co-Organizer of the Main Session on Empowering Global Cooperation on Cybersecurity for Sustainable Development (video https://youtu.be/OItB7LErmFc) *Olusegun Olugbile* reported that participants to the main session, which was held before the BPF workshop, acknowledged a global increase in cybersecurity threats and in exposure to threats. It was recognised that cybersecurity intersects with peace and development and that therefore the IGF is the right place to address the topic. Other issues discussed at the main session were norms and values in cyberspace, human security and the balance between human rights and security, the growing gap in the capacity to protect, the need to improve cyber hygiene, and how a better implementation of existing law could help to secure cyberspace.

BPF Methodology and walkthrough of the draft output document

- *Maarten Van Horenbeeck* gave an overview of the BPF's intersessional activities which consisted of a series of 8 virtual and one in-person meeting complemented with detailed email conversations on the dedicated mailing list. The BPF focused on development and used previous IGF work - the CENB I and CENB II policy options - as starting point to identify security challenges and discuss how to mitigate the risks. A public call for input received 27 formal contributions (ca. 30% more than last year). Special effort was done to reach out to national and regional IGF initiatives (NRIs), amongst other with a dedicated questionnaire. A draft outcome document was published ahead of the IGF meeting and will be completed with insight from the workshop.

  The BPF CENB analysis identified 10 policy areas:

  11. Securing the reliability of and access to Internet services;
  12. Securing the mobile Internet;
  13. Protecting against potential abuse by authorities;

14. Confidentiality and availability of sensitive information;
15. Fighting online abuse and gender-based violence;
16. Securing shared critical services and infrastructure supporting access;
17. Vulnerabilities in ICS technologies;
18. Preventing collected information from being repurposed;
19. Deploy secure development processes;
20. Prevent unauthorized access to devices.

Six additional policy areas were raised in individual contributions:

7. Awareness building and capacity development;
8. Supporting cyber resiliency of cities;
9. Lack of diversity in cybersecurity;
10. Cryptocurrency;
11. Impact of social media on cybersecurity;
12. Whistleblower policies and implementation.

Discussion on detailed policy options

The workshop focussed on two policy areas: safe and reliable access / securing shared critical services, and preventing collected information from being reused for inappropriate purposes / protecting against potential abuse by authorities.

(1) Safe and reliable access / securing shared critical services

- *Cristine Hoepers*, CERT.br, pointed out that the shared critical services that together form the core of the Internet are managed by a large number of organisations that are spread over different sectors and countries. The implementation of best practices and dialogue are essential but challenging as often parties responsible for implementing a best practice (eg IPv6, DNSSEC, etc.) are not the parties that see the benefit throughout. Governments, as big buyers of technology and services, could incentivise by requiring the implementation of best practices by their providers. A second challenge is the availability of secure software. A better education and training of professionals - a role for the Academia - would help to create a workforce with the right competencies and mindset. A better cybersecurity hygiene will improve the ability to face cybersecurity challenges, in particular for SMEs that traditionally have limited budget and resources.

- *Benedict Addis*, the Shadowserver Foundation, warned that domestic legislation intended to improve cybersecurity might have unforeseen consequences and even damage security. He referred to potential perverse effects of obligations to geo-localise content and services, blocking of domain names or the failure to deploy IPv6. The takedown of the Avalanche botnet was a good example of how international cooperation and cooperation between stakeholders leads to success.

(2) Preventing collected information from being reused for inappropriate purposes / protecting against potential abuse by authorities

- *Deborah Brown*, Association for Progressive Communication, stated that in order for technology to enable sustainable development, people, data, networks and devices must be secure. Cybersecurity must be improved so that people trust and use programs and applications that could improve their lives and contribute to sustainable development. The UN Global Pulse Privacy and Data Protection Principles call for reasonable and appropriate technical and organisational safeguards to prevent unauthorised disclosure or breach of data and risk and harm assessment and mitigation steps. Consent is critical for people prone to discrimination.

- *Matthew Shears*, GP Digital, underlined that all policy challenges are interlinked and indivisible. As the world/Internet continues to move towards a more data-rich future which asks for increased security, securing consumer devices becomes a major challenge for their manufactures as well as for the consumers using them. Consumers must be made aware of their responsibility in terms of cyber hygiene and understand the technical security possibilities of the devices they use to connect to the Internet, and help to protect their own security and protect the network itself.

Areas for future stakeholder conversation

The BPF call for contributions asked stakeholders to suggest cybersecuritry areas that would benefit from further stakeholder conversation within an IGF context. The BPF workshop focussed on two of the suggested areas: the need to foster a culture of cybersecurity, values and norms, and the existence of a digital security divide.

(1) A cybersecurity culture, values and norms

- *Alexander Klimburg*, Global Commission on the Stability of Cyberspace, defined norms as not legally binding voluntary agreements that provide soft incentives and disincentives. They can be agreed upon by all kinds of stakeholders, and are not an exclusive instrument of States and governments. He referred to the UNGGE which in 2013 stimulated regional organizations to set up norms and developing an own set of norms in 2015. The recent 'Call to protect the public core of the Internet' by the Global Commission on the Stability of Cyberspace calls upon state and non-state actors not to harm the Internet's public core and damage the stability of cyberspace. The concept of the public core, with an inner and outer core is still being fine tuned.

- *Kaja Ciglic*, Microsoft, stated that the debate on cybersecurity norms cannot be a governments-to-governments discussion, but should include the voice of industry and other stakeholders. Stakeholders should discuss how the UNGGE norms can be implemented and identify additional areas where norms could be beneficial, for example on non-interference in election processes.

(2) The digital security divide

- *Matthew Shears*, GP Digital, warned that the digital security divide could impair the progress made on Internet access.

- *Cristine Hoepers*, CERT.br, explained that in Brazil still only half of the population is online, of which half connects to the Internet via their cell phone. Research has shown that awareness of cybersecurity risks correlates with general literacy. This poses an additional challenge - it is difficult to raise awareness if people do not understand - and increases the importance of better systems and tools.

- *Deborah Brown*, Association for Progressive Communications, pointed out that certain communities are more at risk when data breaches occur, for example those that could fear discrimination based on gender and sexual orientation and gender identity.

Comments and Input from workshop participants

- To increase government participation, the BPF should be aware of what the priorities of governments are use this to define a clear focus for the BPF.
- Companies (incl Apple, Google etc.) are responsible for their own applications.
- A shift is needed from 'security as an afterthought' to 'security by design' to avoid a dramatic expansion of the threat landscape as the number of consumer and network devices rapidly increases.
- The mindset of many IoT companies is still similar to how software developers in the 80s/90s thought about security.

- It's important to collect data on vulnerabilities.
- Consumer protection law will not prevent that IoT devices become part of a botnet.
- Given the importance of email communication for day-to-day businesses, email security and related issues (eg lack of encryption) should be considered by the BPF.
- The IGF intersessional work would benefit from more flexibility in the IGF schedule (eg with multiple sessions) and should better identify and celebrate its successes.
- Cultural gaps between developed and developing regions might complicate the communication around cybersecurity issues.

Annex 4: Summary of the informal BPF Cybersecurity coordination session at the 2017 IGF meeting

Cybersecurity BPF Coordination Session

Thursday, December 21st from 13:30 to 15:00

Room XXVII - E United Nations Office at Geneva (UNOG)

Summary

This session was organized as an outcome of our final Best Practices Forum (BPF) call ahead of the IGF. Several parties expressed an interest in having an informal session to discuss the work of the BPF, rather than simply the subject matter. In particular, we wanted to have an exchange of ideas on where to take the BPF in future years.

During the session, we discussed how the BPF contributes to wider IGF goals by creating a multistakeholder space to collect best practices and experiences around cybersecurity from a wide variety of stakeholders, including by leveraging the National and Regional IGF communities.

This discussion helps build a common understanding between all parties involved, creates an opportunity to exchange views on areas where no consensus exists, and creates a space for learning about topics that are not yet at a level of shared understanding. In addition, the BPF has provided an opportunity to build on previous work within the BPF community, such as the Connecting and Enabling the Next Billion (CENB) work.

In the session, we learned from several government representatives that in order to improve government participation, we would benefit from collecting best practices which everyone should apply, but which may not be universally known or shared. While it was understood that cybersecurity included sensitive issues governments would not be ready to address in an open setting, the representatives of Israel and Switzerland made it clear that they found it essential to engage with non-governmental stakeholders. n addition we should consider leveling up the conversation to a point where the stakes of not participating are higher.

Agenda

This session was organized at the end of the IGF with two main agenda items:

- What issues should be addressed by the broader IGF community?
- What are our priorities for 2018, should the BPF be renewed?

- Looking back at 2017, what worked well? What did not?

The session took place as an additional session, with no transcription, though remote participation was supported and available. A video recording is available at https://youtu.be/owEP5G9hz4E .

The session took place in addition to the main BPF on Cybersecurity session, which was recorded and made available here. A transcript of the main session is available here.

Discussion

Follow up on items from the main BPF meeting

● The session was opened with a comment by David Rufenacht on the current draft document regarding medical devices. Medical devices are sometimes sold on hardware which is only certificate to work with Windows XP, even though that operating system itself is no longer supported. The misalignment between these life-cycles can cause significant security issues, as security updates may no longer be available for the only supported combination. It was suggested this would be a great illustration for the importance of managing a product lifecycle, currently included as a recommendation in the 2017 draft document.

What went well, what did not go very well

● Markus Kummer noted the solid discussion which took place throughout the year. He also noted the draft version of the BPF outcome document is still available for public comment. He also stated that renewal of the BPF is up to the Multistakeholder Advisory Group, but that as a group we can propose a set of issues and themes as paths forward for consideration.

● Maarten Van Horenbeeck noted that this year we had two major challenges we identified:

○ While we hit the ground running generating a proposal for 2017 work, renewal of the group took place in April, so formal work only got started around that time;

○ We saw limited participation from private sector and government.

● Some discussion took place on what makes the IGF a valuable place for the BPF to take place in. The IGF enables countries to move forward, share thoughts and promote better understanding. The BPF in particular promotes global interoperability, creates interfaces for conversation and enables us to develop agreement on limited areas of difference.

● Markus Kummer noted that the value added by the BPF is to bring stakeholders together in an area where they can develop a common understanding, and under one roof, regardless of their background as a stakeholder community.

● Adli Wahid of APNIC noted that there is an opportunity to improve in a few ways:

○ We can engage more closely with the National and Regional IGFs, to increase the input and participation from these communities.

○ The logistical side of this year's IGF made it more difficult to have widespread participation due to the room layouts.

● Markus Kummer and Maarten Van Horenbeeck noted that some outreach had taken place this year to the NRIs, and that there is definitely room for improvement through direct outreach to their meetings. There are also potential opportunities to improve cooperation in the meeting room facilities through the use of electronic queuing mechanisms, though as the location changes from year to year, meeting room use may be different in future years.

● Sivasubramanian Muthusamy noted how the Best Practices Forum must continue to be multi-stakeholder, and is one of only a few opportunities for cybersecurity to be discussed in a public forum. Governments may not always be comfortable discussing cybersecurity in such a public space.

● Paul Wilson of APNIC noted that security has skyrocketed as a concern, including in the Regional Internet Registries. He hopes the Best Practices Forum will continue. Over the last few years he has seen the tone on cybersecurity at the IGF change, from being developmental to being more fear-focused. He sees more space for discussion within the IGF community, and sees potential opportunities for the BPF to help resolve duplication, for instance by creating interconnection with other forums such as the GFCE, which are also working on development and capacity building.

● Markus Kummer noted that the BPF is not a trade-off between security and openness, but that we need to find ways for both to contribute to eachother.

● Winston Roberts, in this forum representing an NGO, but formerly a government representative, noted that governments are often nervous about joining a forum on cybersecurity. We may need to elevate our debate and make it more applicable to their day to day work. In order to do so we'd need to pitch our discussions at a level where the stakes of not participating are clear.

● Amit Ashkenazi of the Prime Minister's Office of Israel noted that many issues are not technical, and several important security solutions are quite simple, such as the requirement to update systems to their most recent patch levels. The BPF could help identify these basic steps that provide a large portion of the value.

● David Rufenacht from MELANI noted how security is a shared responsibility. The government cannot provide it independently. For instance in his example of medical devices, a multi-stakeholder approach is a requirement to properly understand, share and address risk.

Where do we take work next year?

● In the earlier BPF meeting, we raised two areas of possible future development that appeared useful for further investigation:

○ Defining and identifying cybersecurity culture, norms and values;

○ Identifying the risk of a potential digital security divide, between those who have, and those who do not have, access to cybersecurity measures.

● Mike Nelson of Cloudflare participated remotely, noting that the rise in Distributed Denial of Service Attack is an increasing concerns. Countries are increasingly talking about standards to help address the challenge of vulnerable devices. A possible interesting avenue of communication for us could be to collect best practices on how not to build standards. Can the BPF help provide guidance on best practices moving forward on how these standards can be designed and implemented?

● Wout de Natris of de Natris Consult noted how on day 0, he organized a session on "Strengthening cooperation within the context of the IGF: Creating a roadmap for 2018". In this session he investigated what it was that made Private Sector and Government participate in IGF work. The three key reasons were:

○ It fit in with their priorities of what is important work;

○ There is a concrete outcome and a goal;

○ The effort is focused on a single, achievable task.

Based on this, Wout recommends that our effort for future years be more focused, to gain additional traction and engagement. An example of this could be to address the risk of IoT devices by identifying a single action that should be taken, for instance, to ship any IoT device with a unique password, and then working in the BPF to drive all stakeholders to that goal. The goal should have a timeframe assigned to it, for instance "within two years".

● Mike Nelson agreed with the idea to identify best practices: what has worked, where has it worked, where has it not. He also noted that there's value in clarifying terminology - as IGF participants often talk past each other. There could be value in designing some type of taxonomy.

● It was raised in discussion that perhaps outside of trying to define a term, some education could take place on existing terminology, to avoid reinterpretation and changing already established terminology. This could perhaps even include an explanation of the history of the term: where did it come from, and what is it currently being used for -- and how did the term get there?

● Louise Marie Hurel wondered if we could take a topic, such as IoT security, and review it from a cross-cutting way, out of the perspective of each stakeholder group. What would a user-centric approach to IoT security look like, and what can our Best Practices community collect and share from this perspective? We should avoid creating a list of process issues, and coming up with a diagnosis. Instead, we can collect work that has actually contributed and made things more secure.

● Serge Droz from FIRST identified three areas of potential work:

  ○ He noted that taxonomies are useful to define whether something is truly a problem or not.

  ○ There is work to be done on our multi-stakeholder approach, to define the exact responsibilities of each group: who designs, who implements, who regulates?

  ○ He also sees value in noting how different best practices work in unique contexts: for instance, does a particular solution work equally effectively in Africa, or is its use restricted to e.g. EU countries? For what reason?

● Bevil Wooding of the Caribbean NOG gave an example of a project in Belize, where they brought a wide variety of stakeholders together to evaluate cybersecurity implementations. This brought a richness of discussion they had not had before. They developed individual fora for stakeholder groups, and then brought all groups together in a national cybersecurity symposium. In the symposium, they discussed "the same thing at the same time", defining areas and priorities. This then led to the development of a national cybersecurity agenda. They called the positive outcome of this process the "Belize discovery", and it is a best practice they can share.

● David Rufenacht of MELANI noted that IoT as a topic may be too large for the Best Practices Forum, and that the issue of unique passwords is also not valid in all situations: such as when managing objects instead of devices. He does agree with the idea of taking an issue and looking at it from different ways. This can help create stories and real life examples that can be put to work for others.

Other learnings and next steps

● As a next step, we will identify a small number of possible options to move forward, potentially including a cross-cutting look at a specific topic, or the idea of investigating culture, norms and values, or the digital security divide, more deeply. With the group we will start in January by identifying possible new areas of work, and making a proposal, or providing a shortlist of proposals, to the MAG for consideration.

● Wout de Natris noted that we need to do better at reiterating our successes. Things have changed because of the work in the Best Practices Forum. For instance, the BPF on CSIRT documentation was adopted as pre-reading to the GCCS 2015, and at least one CSIRT had been built using the IGF BPF on CSIRT documentation as a guide. Hence the documents we have produced has been useful, and it is important we continue to flag this.

● Anriette Esterhuysen noted she has been following the work of the BPF closely. She believes the secretariat could provide more support by reaching out to member States and making them more aware of the BPF work. However, they are most likely not sufficiently staffed. The Germans, who have shown an interest in hosting the IGF in 2019, could take a strong role in bringing these outcomes to other countries.

- Olusegun noted that we can all become ambassadors of the BPF. In 2017, he brought several Nigerian government delegates to the BPF meeting. In his view, if we bring the BPF outcome documents to Nigeria and work with them to adopt them, we can replicate that work across Western Africa. He also believes we should do more to bring the work to the core government implementers, rather than to policy analysts who may not be practically involved in cyber security.

- Maarten Van Horenbeeck and Wim Degezelle acknowledged there is a tension in terms of next steps between being inclusive of all stakeholder groups, or going more technical and diving deeper. However, that tension is healthy and shows that the group can actually work across multiple areas. Whatever decision we make in terms of progress next year, we will need to be cognizant of these conflicting interests and find a good way forward.