2017 IGF Best Practice Forum on Cybersecurity

All individuals and organizations are asked to kindly try to keep their contributions to no more than 2-3 pages, and are encouraged to include URLs/Links to relevant information/examples/best practices as applicable. When including specific examples or detailed proposals, those may be included as an Appendix to the document. Please attach contributions as Word Documents (or other applicable non-PDF text). https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1

Overview of the call

During 2015 and 2016, the Policy Options for Connecting and Enabling the Next Billion(s) (CENB) activity within the Internet Governance Forum identified two major elements:

❿ *Which policy options are effective at creating an enabling environment, including deploying infrastructure, increasing usability, enabling users and ensuring affordability;*

❿ *How Connecting and Enabling the Next Billion(s) contributes to reaching the new Sustainable Development Goals (SDGs).*

The Best Practice Forum on Cybersecurity realizes that making Internet access more universal, and thus it supporting the SDGs, has significant cybersecurity implications. Well-developed cybersecurity helps contribute to meeting the SDGs. Poor cybersecurity can reduce the effectiveness of these technologies, and thus limit our opportunities to helping achieve the SDGs.

BPF participants have conducted an initial study of how the policy proposals compiled as part of CENB Phase I and II may affect, or be affected by, cybersecurity implications.

As part of this ongoing effort, the IGF is now calling for public input to collect additional risks and cybersecurity policy recommendations that can help mitigate security impacts, and help ensure ICTs and the Internet continue to help contribute to achieving the SDGs.

About APC

The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 that wants everyone to have access to a free and open internet to improve lives and create a more just world. apc.org

Contact: Mallory Knodel, mallory@apc.org

Association for Progressive Communications submission to output document for presentation by Secretariat

Good cybersecurity reinforces human rights. From the Freedom Online Coalition working group “An Internet Free and Secure, “Cybersecurity and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security. Recognizing that individual security is at the core of cybersecurity means that protection for human rights should be at the center of cybersecurity policy development. Such an approach is instrumental in reminding policy-makers that cybersecurity must take into account individual security and human rights and that, as a consequence, cybersecurity policies should be human rights respecting by design.”[1]

How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Technology can be an enabler of all SDGs, however in order for information and communication technologies (ICTs) to be leveraged fully for sustainable development, data, networks, devices, and most importantly people 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. This is especially true for very sensitive personal information such as biometrics, health, and other data that is collected about populations and communities, for the provision of goods and services to help achieve the sustainable development goals. It is critical to implement good cybersecurity practices in order for people to trust and participate in initiatives to achieve the SDGs and for those initiatives to be trusted and successful. The UN Global Pulse’s Privacy and Data Protection Principles for harnessing big data for development and humanitarian action provide some guidance in this regard. In particular, the Principles call for reasonable and appropriate technical and organisational safeguards are in place to prevent unauthorised disclosure or breach of data, and for risk and harm assessment and risk mitigation processes before any new or substantially changed project is undertaken to ensure that the risks and harms are not excessive in relation to the positive impact of the project.[2]

How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

There are several ways in which cybersecurity measures are insufficient to protect people. Insufficient design and execution as well as intentional but harmful policies and practices that put data at risk such as encryption backdoors, failing to disclose known exploits and vulnerabilities, national intelligence programmes without oversight, criminalisation of technical experts and researchers, undermining

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

[2] “Privacy and Data Protection Principles.” UN Global Pulse. http://www.unglobalpulse.org/privacy-and-data-protection

standards and protocols.

Poor cybersecurity can result in damages to people and erodes trust. Data at risk is people at risk. It is not hyperbole to say that poorly secured digital initiatives to achieve SDGs can do more harm than good.

In the 2016 IGF workshop on internet of things, a panelist remarked, “Governments undermine their efforts towards security when they are seen violating cybersecurity with surveillance. If government hacking is on the front page of newspapers around the world, efforts to secure the public's use of SDG supporting technical tools are going to falter. We know often these are different departments or ministries who are responsible for ICTs versus intelligence or national security. So there needs to be within local contexts norms and policies that work together, not at cross purposes.”[3] Further noting that ministries responsible for sustainable development are often different than those that deal with national security.

Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:

Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services; Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments; Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended; Confidentiality and availability of sensitive information, in particular in medical and health services; Use of information collected for a particular purpose, being repurposed 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; Unauthorized access to devices that take an increasing role in people’s daily lives

It is important to support efforts to mitigate DoS 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 continue to develop protocols that cannot be used for exploits such as DDoS, to the extent possible.

In terms of policy, governments must ensure that solid technology practices such as bug bounties are encouraged, not discouraged, and that they are not using their power to actively contribute to the problem by hoarding vulnerabilities or creating backdoors to secure communications technologies, as

[3] http://www.intgovforum.org/multilingual/es/content/igf-2016-day-2-room-9-ws35-harnessing-iot-to-realize-the-sdss-what%E2%80%99s-required

examples. Governments must regulate the private sector through data protection laws and other consumer protections. They must pursue policies or treaty options that compel signatories to abide by international principles, norms and standards that ensure cybersecurity and national security measures that employ digital technology are necessary and proportionate. Governments should be transparent in, and protect disclosures by the private sector about, partnerships between the private sector and governments.

The private sector has a responsibility to respect human rights, including the right to security, by acting with due diligence to avoid infringing on human rights and addressing adverse impacts with which they are involved. To meet this responsibility, the private sector must correctly implement protocols, standards and best practice in technology development from accessibility standards on the web to properly hardening internet infrastructure at the lower levels of the internet. They must alsocreate clear and readable terms of use for users, and proactively inform users of software updates in order to fix critical vulnerabilities,.

Academics and other security experts should monitor security best practices by all stakeholders. There should be policy protections for researchers that seek out vulnerabilities in technology in the public interest.

Online abuse and gender-based violence

States must respect, protect and fulfil women's rights by fully implementing CEDAW at the national level through laws and policies. States – and in particular legislators – must pursue a preventive and proactive approach to GBV. This includes the adoption of policies and programmes addressing and incorporating the issue of GBV at all levels and ensuring *the full rights of all women – particularly survivors of GBV*. States should recognise GBV as a human rights violation and provide a comprehensive definition of GBV that includes psychological violence and recognises its occurrence in both public and private life. The perception of GBV as a moral issue rather than as a form of discrimination against women reinforces control over female sexual behaviour and punishes women who transgress sexual norms. Additionally, it is crucial that any technology-related GBV laws take into account the gendered nature of the violation and addresses it as a social phenomenon.

Gender-unequal access to technology and women's subordinate status in the ICT arena (and society at large) are realities that must be confronted. States should address the gender divide in relation to ICTs by taking affirmative action, such as providing subsidies for ICT-related courses for women and girls, and in particular marginalised groups of women. Comprehensive capacity building – including rights-based education – should be undertaken by all institutions. This should specifically address gender issues and women's rights. In particular, companies should take a rights-based approach and adopt the Women's Empowerment Principles.[4]

Internet governance platforms and forums should provide a mechanism to ensure women's meaningful participation in policy discussion and decision making. Women's organisations and activists should be

[4] http://weprinciples.org/Site/PrincipleOverview/

encouraged to proactively participate in internet governance and take on leadership roles to influence the agenda and shape public policy matters on internet governance.

Adequate budgets and resources should be allocated by states to address GBV. These should be directed towards making the institutions involved in addressing GBV functional and able to effectively address the needs of women survivors of violence. States should, where possible, create a dedicated agency to receive and investigate complaints of GBV.

In developing policies to respond to reports of abuse, intermediaries should consider social context and understand essential differences in violence and gender-based abuse and address the English language bias in reporting mechanisms. While the primary content may be available in many languages, the reporting mechanisms are not available in all user languages and both staff and systems appear incapable of processing multilingual requests. Critical to these points is increasing diversity at all staff levels.

Intermediaries should have minimal obstacles in taking down pages, posts, or content in relation to privacy concerns specifically when accompanied by threats, and ensure systems-wide removal of individual content (photos, videos, tweets). If companies fail to take action, there should be clear accountability measures necessitating at least a clear response to complainant. They should reserve the right to terminate accounts specifically on the basis of repeated gender-based harassment, hate and abuse.

Companies should use the following points to improve their reporting mechanisms:

- Legitimate: the mechanism is viewed as trustworthy and is accountable to those who use it.
- Accessible: the mechanism is easily located, used and understood;
- Predictable: there is a clear and open procedure with indicative time frames, clarity of process and means of monitoring implementation.
- Equitable: it provides sufficient information and advice to enable individuals to engage with the mechanism on a fair and informed basis;
- Transparent: individuals are kept informed about the progress of their matter;
- Rights-respecting: the outcomes and remedies accord with internationally recognised human rights;
- Source of continuous learning: the mechanism enables the platform to draw on experiences to identify improvements for the mechanism and to prevent future grievances.

Intermediaries should also provide greater transparency and accountability regarding (in)action on content and privacy requests and greater transparency on the departments and staff responsible for responding to content and privacy complaints. The best way for companies to improve their approach to GBV is to engage with experts in gender, sexuality and human rights to provide input into policy formation, staff training, and education/prevention programs.

The focus of responses to GBV must be on redress rather than criminalisation, and particular attention must be paid to *the provision of effective protective orders and the availability of support services*. Practical means should be provided to survivors to halt violence without requiring them to become embroiled in lengthy and demanding criminal procedures. Due to the transnational nature of many cases, policies should promote Mutual Legal Assistance Treaty (MLAT) reform to increase access to justice.

The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis

We point to the best practice of developing with free/libre and open software principles that allow for transparency of code as well as the security benefits of audits and code reviews from third parties as well as community contributions to fix bugs and employ best practice implementation of technical standards.

Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity. This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

Indeed coordination and cooperation between stakeholders is needed as technology development and use is complex, and goes beyond simple producer-consumer or -user relationships. Enjoyment of rights is the biggest enabler of internet use and development, so this must be a priority for all stakeholders in their respective roles.

Governments must regularly engage a diversity of experts from civil society, academia and the private sector to set regulations that prioritise human rights, including the right to security and privacy, and data protection.[5]

The technical community must also recognise and broaden its implicit values to set standards and protocols that protect human rights by design. Achiving this means including a diversity of expertise and experience in its standards bodies.[6]

According to the UN Guiding Principles on Business and Human Rights,[7] corporations have a responsibility to respect human rights, including the right to security and privacy, by conducting due diligence to avoid infringing on human rights and addressing adverse impacts with which they are involved. In the context of cybersecurity, this requires companies to help create and follow regulations

[5] Tunis Agenda for the Information Society. (2005). http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[6] https://www.apc.org/en/pubs/human-rights-and-internet-protocols-comparing-proc

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

that improve cybersecurity and implement protocols and standards.

Civil society brings relevant expertise and connection with the people who use technology, which means they play an important role in bringing the security concerns of internet userst to policy and technical debates, and can help build awareness and skills among internet users to improve their own security. .

What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?

We believe best practices in technology development, from policy to design to use, is the most important issue that should be addressed by the forum. We recommend research and publication of best practice case studies on these or other related topics:

- ❿ Software that correctly implements secure standards and protocols;
- ❿ Free/libre and open source software development;
- ❿ Third party code auditing;
- ❿ Feedback loops between software implementers and protocol and standards setting bodies;
- ❿ Strong rights-enabling cybersecurity and cybercrime policies and laws;
- ❿ Protecting technical and security experts and researchers from criminal prosecution.

Technical experts from a variety of contexts (FLOSS development, for example) need to be part of the conversation in order to share their practices. It would be important to involve experts/academics in software development who have studied and compared different approaches to development. Lastly, due to the criminalisation of technical experts, criminal defense lawyers would be a welcome addition to the forum.

References

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

Kaye, David. Report to 29th session of the Human Rights Council. (2015) HRC. https://www.justsecurity.org/wp-content/uploads/2015/06/Kaye-HRC-Report-Encryption-Anonymity.pdf

NETmundial Multistakeholder Statement. (2014, 24 April). http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

See Human Rights Council Resolution 20/8 (2011) on “The promotion, protection and enjoyment of

human rights on the Internet” http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

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

“Extracting lessons from NETmundial: Achieving bottom-up and multistakeholder outcomes from global internet policy governance discussions.” (July 2016). APC https://www.apc.org/en/pubs/achieving-bottom-and-multistakeholder-outcomes-glo