# Report of the BPF Cybersecurity workshop 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:

  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 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.

***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.