BPF on Cybersecurity

Internet Governance Forum – Geneva

Agenda

Time	Activity
15:00	Introduction of panelists and the Best Practices Forum on cybersecurity
15:10	Summary of the main session on cybersecurity
15:15	Walkthrough of policy options
15:25	Discussion of two policy areas and discussion with panelists and attendees • Safe and reliable access / securing shared critical services • Preventing collected information from being reused for inappropriate purposes / protecting against potential abuse by authorities
16:00	Discussion of valuable work for the BPF in future years • Culture, Values and Norms • Digital Security Divide
16:20	Finalize discussion on 2018 topics
16:30	Ending

Introduction of Panelists

- **Deborah Brown**, Association for Progressive Communications
- **Matthew Shears**, GP Digital
- **Benedict Addis**, Shadowserver
- **Alex Klimburg**, Global Committee on the Stability of Cyberspace
- **Kaja Ciglic**, Microsoft
- **Cristine Hoepers**, CERT.br

BPF on Cybersecurity

- **Goal setting:** identify cyber security policy options that help achieve Connecting and Enabling the Next Billion and support the SDGs
- Detail **risk analysis** of CENB Phase I and Phase II work
- Call for **Focused Contributions**
  - Distribution of main questionnaire
  - Distribution of NRI-focused questionnaire
- Series of **8 virtual and one in-person meeting** at the GCCS

BPF on Cybersecurity

- **Detailed e-mail conversations**
  - Industry responsibilities and Duty of Care
  - Hacking back
  - Forums working on Internet of Things security
  - Cyber norms and Confidence Building Measures
  - Internet shutdowns
  - Definition of cybersecurity
  - Engaging private sector and government

BPF on Cybersecurity

- Focused contributions
  - 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)?
  - 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)?
  - 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, these cyber security challenges?

BPF on Cybersecurity

- Focused contributions
  - 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.

    Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

  - 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?

Formal contributions

- **Mr. Shredeep Rayamajhi**
- **Mr. Ben Wallis**, Microsoft
- **Dr. N. Sudha Bhuvaneswari**
- **Mr. Foncham Denish Doh**, Cameroon Internet Governance Organization
- **Mr. Ji Haojun**, Government of China
- **United Nations Cuban Association**
- **Ms. Anita Sohan**, Commonwealth Telecommunications Organization
- **Mr. Mohit Saraswat**
- **Mr. Akinremi Peter Taiwo**, African Civil Society on Information Society
- **Mr. Peter Micek**, Access Now
- **Mr. Naveen K. Lakshman**

Formal contributions

- **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 Muthasamy**, Internet Society, Chennai Chapter

Formal contributions

- **Ms. Raquel Gatto**, ISOC
- **Mr. Nigel Cassimire**, Caribbean IGF
- **Mr. Arzak Khan**, Internet Policy Observatory Pakistan
- **Ms. Mallory Knodel**, Association for Progressive Communications (APC)
- **Ms. Tatiana Tropina,** EuroDIG

Report from the main session

Walkthrough of 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

Walkthrough of additional policy areas

These areas were raised proactively in individual formal submissions.

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

- Safe and reliable access / securing shared critical services

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

Areas of future stakeholder conversation

- **Fostering a culture of cybersecurity** and **core values**

- **Technical issues**
  - Internet of Things ecosystem security
  - Vulnerability of critical infrastructure and internet resources
  - DoS/DDoS attacks, BGP/IP prefix hijacking and DNS abuse
  - Cybercrime and ransomware
  - Cognitive computing and artificial intelligence
  - Mobile network security
  - Anti-abuse initiatives
  - Lack of education and end user awareness

Areas of future stakeholder conversation

- **Policy and governance issues**
  - Development of internationally agreed upon cyber norms
  - Framework to foster international cooperation and legal principles
  - State stability and peace in cyberspace
  - Increase awareness of risk management processes
  - Awareness of criminal justice practices

Possible work areas for 2018

- **Culture, values and norms**

  A need exists to foster a culture of cybersecurity, making sure it is understood by each stakeholder group, and identifying a core set of values. This can be used to assess, debate and improve on cyber security norms.

- **Digital Security Divide**

  The gap between those who have access, and those who have not, is closing. However, the gap in access to security measures, both between individuals (wealthy and poor) and states (developing vs. developed) could be a continuing challenge, creating disparities in economic opportunities.

Thank you!

- **IGF Geneva Coordination session for future work**
  Room XXVII on Thursday 21 December, from 13.30 to 15.00

- **Document open for public input**
  https://www.intgovforum.org/multilingual/content/igf-2017-best-practice-forum-on-cybersecurity

- **Join our mailing list**
  http://www.intgovforum.org/mailman/listinfo/bp_cybersec_2016_intgovforum.org