IGF 2021

Best Practice Forum

Cybersecurity

on the use of norms to foster trust and security

Update to the IGF Open Consultations and MAG Meeting

Wednesday 29 September 2021

BPF webpage

https://www.intgovforum.org/multilingual/content/bpf-cybersecurity

BPF Background

- **Cybersecurity BPFs at the IGF**
  - Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics.
  - In the past 3 years the BPF explored the concept of culture, norms and values in cybersecurity, with an evolving focus:
    - BPF 2018: importance of norms as a mechanism in cybersecurity for state and non-state actors
    - BPF 2019: international cybersecurity agreements
    - BPF 2020: lessons to learn from global norm initiatives unrelated to cybersecurity / UN cyber norms reflected in international cybersecurity agreements
- **2021 focus and work plan**
  - WS1: Mapping of cybersecurity agreements (continuation of last year's work and deeper dive into the drivers of cyber norms).
  - WS2: Testing norms concepts against Internet events.
  - WS3: Outreach and cooperation with other IG(F) initiatives.
- **Meetings and next steps**
  - Next BPF CS Update call: Thursday 14 October at 6:00 am UTC.
  - BPF Cybersecurity workshop @IGF2021

    Friday 10 December, 11:15-12:45 CET / 10:15-11:45 UTC

IGF 2021

Best Practice Forum

Cybersecurity

on the use of norms to foster trust and security

Work stream 1:

Mapping of cybersecurity agreements

What?

- Continuation of the BPF's mapping exercise
- New agreements and revisiting already analyzed agreements
- Focus on drivers of cybersecurity norms

Update on activities work stream 1

- **Scope – agreements selected that include following elements**
  - Specific commitments or recommendations that apply to any or all signatory groups
  - Commitments or recommendations must have a stated goal to improve the overall state of cybersecurity
  - Agreement must be international in scope, must have multiple well-known actors that operate significant parts of internet infrastructure, or are governments
  - The agreement must include voluntary, nonbinding norms for cybersecurity, among and between different stakeholders.
- **Update**
  - The WS identified **36 agreements** based on the above scope and agreed on 26 norm elements for the analysis
- **Ongoing and next steps**
  - Analysis of the 36 agreements
  - Additional research on the '**intended impact of the 11 UN norms for responsible state behavior online**.'

IGF 2021 Best Practice Forum Cybersecurity

on the use of norms to foster trust and security

Work stream 1: **Mapping of cybersecurity agreements – list of agreements**

G20 Antalya Summit Leaders' Communiqué; G7 Charlevoix commitment on defending Democracy from foreign threats; G7 Declaration on Responsible States Behavior in Cyberspace; Cybersecurity Tech Accord; Freedom Online Coalition's Recommendations for Human Rights Based Approaches to Cyber security; Shanghai Cooperation Organization's Agreement on cooperation in the field of ensuring the international information security; African Union Convention on Cyber Security and Personal Data Protection; Council to Secure the Digital Economy International Anti-Botnet guide; League of Arab States Convention on Combating Information Technology Offences; East African Community (EAC) Draft EAC Framework for Cyberlaws; Economic Community of Central African States (ECCAS) Declaration of Brazzaville; NATO Cyber Defence Pledge; EU Joint Communication: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU; Mutually Agreed Norms for Routing Security (MANRS); Southern African Development Community Model Laws on Cybercrime; Paris Call for Trust and Security in Cyberspace; UN Group of Governmental Experts (GGE) on information security combined consensus reports from 2010/2013/2015 – "The Framework for Responsible State Behavior in Cyberspace"; Siemens Charter of Trust; GCSC's Six Critical Norms; Commonwealth Cyber Declaration; World Wide Web Foundation's Contract for the Web; Ethics for Incident Response and Security Teams (EthicsfIRST); APEC Guidelines for Creating Voluntary Cyber Security ISP Codes of Practice; Organization of American States List of Confidence- and Security-Building Measures (CSBMS), DNS Abuse Framework, BRICS Summit (2015-2020); OSCE CBMs (2013, 2016); 2015 ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies; ASEAN-United States Leaders' Statement on Cybersecurity Cooperation; 2021 GGE final Report; Freedom Online Coalition (FOC) joint statement on the human rights impact of cybersecurity laws, policies and practices; (Concept) Convention on International Information Security; International code of conduct for information security; G7 Charter for the Digitally Connected World; ITU Resolution 50 – Cybersecurity; OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity; Digital Geneva Convention.

IGF 2021

Best Practice Forum

Cybersecurity

on the use of norms to foster trust and security

Work stream 2

Testing norm concepts against Internet events

What?

- Research question: *How are norms effective at mitigating adverse cybersecurity events ?*

Update on activities work stream 2

- **Update**
  - WS 2 determined criteria for choosing a representative spread of cybersecurity incidents for a literature review and landed at **10 cybersecurity incidents**.
  - Researchers used secondary sources to answer the research question and evaluated if qualitative research in the form of interviews with those affected by the cybersecurity event would enhance their analysis.
  - WS 2 shortlisted cybersecurity events for further qualitative analysis.
- **Ongoing and next steps**
  - Qualitative analysis – WS 2 is identifying and reaching out to potential interviewees representing parties affected by the shortlisted cybersecurity events.
  - Additional research on the '**intended impact of the 11 UN norms for responsible state behavior online**.'

IGF 2021 Best Practice Forum Cybersecurity

on the use of norms to foster trust and security

Work stream II: **Testing norm concepts against Internet events – list of cybersecurity events analyzed**

CIH virus
Estonian DDoS attacks
Ghostnet
Stuxnet
Snowden disclosures
Heartbleed
NSO Group’s Pegasus
Aadhar data breach
Brazil’s Superior Electoral Court
Solarwinds

IGF 2021

Best Practice Forum

Cybersecurity

on the use of norms to foster trust and security

Work stream 3:

Outreach and cooperation with other IG(F) initiatives

What?

- Drive engagement and participation in the BPF
- Better integrate BPF work in the IGF Programme and activities

Update on activities work stream 3

- **Update on activities**

28 June – EuroDIG 2021 **Presentation and update of the BPF Cybersecurity** (session Towards an innovative IGF 2021)

8 Sept - **Capacity workshop - Effective national cybersecurity policies and strategies linked to the UN Sustainable Development Goals** (IGF 2021 OUR DIGITAL FUTURE series).

Cooperation with the **IGF MAG Issue team Trust, Security, Stability** on preparations for the session during the IGF Preparatory and Engagement phase, and the Main session at IGF 2021.

Upcoming

30 Sept – Paris Call Working Group on Advancing Cyber Norms

8 October – AfriSIG

(date to be confirmed) - LetsTalkCyber

Outreach opportunities for the BPF ?

Share with us and the WS 3 will follow up!