TRUST

Trust in the online world is a prerequisite for the Internet to develop its potential as a tool for empowerment, a channel of free speech and an engine of economic development. In this context, trust relates to the security, stability, and resilience of the infrastructure, systems and devices, and also to the need for people to be safe and secure. These are both vital elements for enabling a healthy and empowering digital environment, beneficial to all.

Commented [BW(1]: Minor comment – Trust WG had not yet concluded discussion as to the best verb here, e.g. develop, realize, unleash.

This thematic track is an evolution of the discussions under the IGF 2019 track on Security, Safety, Stability & Resilience, which are summarized in the Berlin Messages. It will provide opportunities to discuss strategies and best practices for protecting both systems and users, along with the appropriate roles and responsibilities of governments, industry and other stakeholders, while taking into account multidisciplinary perspectives. The track will also allow for a consideration of the relationship between security and people's fundamental freedoms and rights, exploring where the balance might be struck or trade-offs might be needed in response to the growing range of threats to the global Internet and to Internet users from all age groups.

Bulleted list of related tags/issues and illustrative policy questions

1) Cybersecurity policy, standards and norms

Tags: Cybersecurity Best Practices, Norms, Cyber-crime, Cyber-attacks, capacity development, confidence-building measures

Policy questions:

- Which policy measures could be taken for the protection, prevention and defense against cyber threats?

- What is the role of cybersecurity norms, do they need to be strengthened, and how can their implementation be assessed?

- What role should different stakeholders play in cybersecurity capacity building approaches?

2) Security, stability and resilience of the Internet infrastructure, systems and devices

Tags: IoT, Domain Name System, DNS abuse, DNS security, Internet protocols, encryption, global routing security

Policy questions:

- What role could and should end-to-end encryption play in strengthening security and privacy? How could end-to-end encryption on the other hand impede the identification of criminal activity?

- What can users and other stakeholders do to mitigate the impact of DNS fraud and abuse?

- How can network operators and other stakeholders effectively contribute to eliminate unreliable or false routing information?

- How can governments focus more on reliability and redundancy? What are best practices in that area (at all layers of the stack: reliable routing of Internet traffic, transport, DNS, security, Content Distribution Networks, Web, applications like social media, e-payments)?

- What role can standards and policy harmonization play in improving IoT Security?

- How can open standards support network resilience and critical servers e.g. time servers and DNS servers?

- What role can the implementation of the principles of safety by design, privacy by design and by default as a principle play to secure human rights and achieve increased safety?

3) Digital Safety to enable a healthy and empowering digital environment for all

Tags: Human rights, digital safety, child online safety, CSAM, hate speech, extremist content, terrorism, social media platforms, freedom of expression online

Policy questions:

- What are the responsibilities of digital platforms and public authorities in regulating or policing content, and where and how should the balance be struck between freedom of expression and public safety?

- How should governments, online platforms, civil society and other stakeholders work together to fight dangerous content online and tackle the misuse of the Internet for the exploitation of children and dissemination of extremist violence and terrorism?

- Do, or should, governments regulating online content have a duty to conduct human rights impact assessments and multi-stakeholder consultations to address the impact on freedom of expression and other human rights?

- In what ways might encryption and related technologies threaten online safety or, paradoxically, foster trust in electronic communications?

- How can risks of poor conduct and malicious content (including violence against women, children and all vulnerable groups) be addressed successfully through legal and regulatory approaches as well as by technical instruments, and how can digital civility be increased?

4) Trust, Media and Democracy

Tags: disinformation, fake news, deepfakes, hate speech, freedom of expression online, democracy, elections, hacking

Policy questions:

- Disinformation / “fake news” and deepfakes pose and threats to the integrity of journalism; how can technology help to tackle them and restore trust?

- What kind of collaboration among Internet platforms and media outlets could work to fight disinformation and fake news online?

- What role can technologies play in protecting democracy (e.g. robust electronic voting) and threatening democracy (e.g. hacking of voting, concealed influencing of voters, dissemination of political disinformation)?

5) Trust and identity

Tags: facial recognition, biometrics, digital identity, decentralized identities, blockchain, bias, e-banking, e-health, AI, business models

Policy questions:

- How should we address the potential for AI technologies to wittingly or unwittingly be used in ways that adversely impact vulnerable populations or certain groups of society?

- How can regulation be crafted to tackle undesirable behaviour without restricting beneficial uses of AI or undermining incentives for innovation?

- How can we ensure trust in medical confidentiality in the digital age?

- What approaches exist for ensuring the safe and unbiased use of facial recognition and biometrics?

- What can be done to address lack of trust in some Internet business models?

6) Fragmentation / sovereignty

Tags: tech nationalism, Internet shutdowns, digital sovereignty, jurisdictions, trans-territorial regulations

Policy questions:

- How can we overcome increasing fragmentation in cyberspace at national, regional and global levels?

- What is digital sovereignty, is it positive or negative, and how are national and international laws applied in cyberspace?

- What are the impacts of trans-territorial regulations regarding digital sovereignty, and how the national and international laws may be applied in cyberspace, preventing fragmentation?

Associated Sustainable Development Goals (SDGs): **3**, **5**, **9**, **16**

Commented [BW(2]: There is an open question here about how best to represent this issue, which came up in Berlin and in the responses to the Call for Validation.

Jutta says that this is a cross-cutting issue which relates not only to Trust but also to the other tracks.

It is not clear how that could be accommodated within the four-theme structure of IGF, and under which tracks / in which ways we might invite the community to make proposals on this topic.

One solution might be to:
-put these issues under sub-theme “2. Security, Stability and Resilience of the Infrastructure…”, in terms of how Internet shutdowns and assertions of digital sovereignty could impact the cohesion of the Internet’s infrastructure.
- allow for fragmentation / sovereignty issues to also appear under other themes (e.g. impact on data flows under Data and impact on ability to access knowledge / information under Inclusion

Commented [BW(3]: It would be useful to get the MAG’s views on whether this overlaps with the data track and is suitable to include here