IGF Internet Governance Forum

IGF BERLIN 2019

Security, Safety, Stability and Resilience

About the Theme

At IGF 2019, discussions on this theme considered:

- The vital role of cybersecurity and online safety as prerequisites to economic growth and a healthy digital environment beneficial to all.
- Stability and resilience of the infrastructure.
- Safety of the users of digital technologies and applications.
- Multidisciplinary perspectives to protect both systems and users.
- Through multistakeholder and multidisciplinary cooperation gaining a better insight in the multidimensional aspects, risks, threats and different ways to address them.
- The importance of stakeholder collaboration in responding effectively to the growing range of threats to the global Internet and its users, while preserving the benefits we enjoy.

Berlin IGF Messages on Security, Safety, Stability and Resilience

Safety and Security Online

- The Internet will only achieve its potential as a channel of free speech and an engine for economic growth if it remains a safe place where people feel secure. Any cybersecurity approach must seek to preserve the benefits people enjoy while tackling the risks. This calls for holistic approaches to protect online users while building or keeping their trust in using the Internet.

- Tackling hate speech is a shared responsibility of stakeholders. Different opinions on mechanisms or instruments should not stand in the way of working together towards a clearer and shared understanding of hateful content.

- Security and people's fundamental freedoms and rights can coexist, but sometimes there need to be trade-offs. However, prioritizing security over people's freedoms and rights, including freedom of expression and privacy, must be legitimate, proportionate, and based on the rule of law.

- Discussions on online safety need to rely on robust data.

- Children's rights are no different in the online or offline world – in particular their rights to play and their rights to protection from inappropriate, illegal and bullying behaviours as well as their rights to be protected from sexual abuse and commercial exploitation. Making the Internet a safer environment for children can only be achieved by a diversity of measures and through collective responsibility, including recommendations for parents and caretakers to guide their children cope with potential risks and harms.

- The international multistakeholder community needs to accurately define scope and terminology of issues on disinformation and interference of electoral processes, and to have a common understanding of what is considered acceptable and responsible behaviour and to make progress on capturing and raising awareness of accepted norms.

- Achieving safety online requires involvement of stakeholders at different levels. Industry players and stakeholders should explore what is tangible and achievable when it comes to gathering and sharing information to prevent online abuse. A shared understanding amongst all players can lead to agreement on ways to act and cooperate.

- Strengthening digital and media literacy is key to combatting the online and real world harms of the distribution of online misinformation. Strengthening people's capacity to protect themselves, adapt and become resilient is key to minimizing the harmful effects of cyberbullying.

Security of the Infrastructure

- While the current trend to tackle illicit or abusive content is to cancel, transfer, delete or suspend domain names via the Domain Name System seems like a quick and easy solution, it does not provide an effective and sustainable way to remove malicious content.
- Online platforms and providers, while taking appropriate measures to delete or block illegal content, should also reach out to and cooperate with law enforcement agencies to provide information for preventive measures. Policy makers and responsible parties should gain more insight in the possibilities and limitations of technical measures solutions through collaborative multistakeholder partnerships.
- More than a quarter of the Internet's traffic now runs on IPv6. Stakeholders need to continue engaging and collaborating, so that this important transition continues to happen.

Policy and Cooperation

- The future of the Internet is a shared responsibility. Multistakeholder and multidisciplinary dialogues are the most appropriate ways to find policy solutions and to identify physical world implications of behaviour and policy decisions in the online space.
- For multistakeholder dialogue to evolve into effective consensus building and, finally, effective and predictable policy implementation, it would be helpful to standardize definitions and terms.
- A safe space in dialogue and policy-making to disagree, to dissent and to protest should be preserved as it provides a valuable opportunity to achieve better outcomes, to correct course and to learn from each another.
- Norms become embedded in behaviour over time. When actors feel the need to hide their behaviour from others, it is an indication that a norm has become established. Every effort to pursue what is considered proper behaviour contributes to establishing community-wide supported cybersecurity norms. This process benefits from the creativity of a multistakeholder and multidisciplinary approach.
- The pace of technology development is outpacing traditional processes to put in place policy and regulatory processes to address security issues in a timely way. It is necessary to enhance collaboration to develop and implement policy solutions, and for norm development processes to be inclusive and respecting human rights.
- Amidst the current atmosphere of escalating tensions between countries in cyberspace, resulting in the development of increasingly sophisticated cyberweapons, both defensive and offensive, it is ever more important to pursue effective confidence building measures (CBMs) to establish trust and promote global stability online.

Capacity building

- We need to foster a more informed dialogue between stakeholders, based on a better understanding of the technical, legal and economic feasibility of the various digital sovereignty models being considered or implemented around the world as well as their implications for Internet governance.
- Internet users have an obligation to contribute to their personal security online. However, they can only be expected to act as responsible users if they understand what is at stake, are aware of the risks, know their rights, and have learned how to act. Users, in particular children, need to be empowered. Cybersecurity training and capacity building should enable all users, including the more vulnerable groups and minorities, to become more secure online and able to demand and defend their human rights safely.
- Significant opportunities exist to improve the global ecosystem security through meaningful actions that promote trust and increase capacity among nation states, and between states and other stakeholders. There are various forums, including the IGF, and initiatives for multilateral, regional and bilateral engagement, where states can build up relationships, exchange experiences and learn from innovative new approaches.
- There is a need for curated, accurate information on security and safety best practices to be localized in many languages.