IGF Internet Governance Forum

The Internet of Trust
INTERNET GOVERNANCE FORUM
PARIS, 12–14 NOVEMBER 2018

IGF 2018 Messages - Cybersecurity, Trust and Privacy

Overarching messages

All stakeholders agree on the importance and relevance of cybersecurity. Only a secure and reliable cyber space can generate and preserve trust in the Internet. With the development of the Internet and new technologies, the cybersecurity question has become more complex, translating into a wide range of angles and issues and engaging a multiplicity of players. Privacy, data protection, and the security of new technologies, are among some of the issues that are central to the cybersecurity dialogue.

Trust & Stakeholder cooperation

- Cybersecurity and privacy are often intertwined and interdependent. They impact the trust in the digital space and may limit its potential for growth and prosperity. Cooperation based on mutual recognition and successful models of engagement between governments, the private sector, technical community and the civil society, can address privacy and cybersecurity concerns without undermining the open, free and secure nature of the Internet.
- A holistic view on cybersecurity that addresses technical as well as economic-socio-cultural elements within countries and organisations is important. Risk management and multistakeholder processes are crucial to start the conversation, in working together and building trust.
- Strengthening multistakeholder cooperation on cybersecurity capacity building is increasingly recognised as a major challenge. Joint engagement among government actors, the private sector, and civil society should be the basis for more effective, strong and sustainable public-private-civil partnerships.
- Security is a task for all stakeholders, including individual users. Informed users, aware of the risks and conscious of their behaviour, will take better decisions when active online. Too often however, too much responsibility is put on the shoulders of end-users, who are identified as part of the risk or threat, when instead, cybersecurity measures should be focused on protecting people.

Cyber Diplomacy

- Cyber stability is a common goal for State and non-State actors - because without it, the benefits of cyberspace and the future of the digital economy will be jeopardized. Stakeholders need to recognise the highly complex and transfrontier character of cyber threats, and undertake appropriate international cooperation, share information and pursue norms of responsible behaviour.
- A combination of diplomatic efforts and confidence building measures can contribute to preventing cyber conflicts between States, while non-binding voluntary norm-building for State behaviour in cyberspace serve as essential guides.
- States have legal and ethical responsibilities in ensuring cyber stability. Policy initiatives, controls on the proliferation of cyber arms, and their commitment to the Call to Protect the Public Core of the Internet contribute to cyber stability.
- Developing a cybersecurity strategy requires a multistakeholder and multidisciplinary approach. While all have a common interest in having a stable and safe cyberspace, each stakeholder has its own, but complementary, responsibilities.

- The cyberspace is different, but not separate from, the real world. Therefore, the existing principles that together form the basis of our world and societies, should be recognised as basic principles in Internet governance, in combination with specific answers for challenges inherent to cyberspace.

Data Privacy & Protection

- Institutional solutions adopted in countries in the Global North to reconcile the protection of privacy and access to data to address digital threats affect the entire Internet ecosystem, and may therefore have implications for countries in the Global South. There are opportunities for the creation of legal interoperability frameworks between developed and developing countries in a mutually-agreeable and negotiated way.
- Enhanced digital identity management must increase data privacy, in particular where data-sharing is made mandatory under national digital identity programs. Personal data must be protected from hacks and misuse, and tracking and monitoring of users must be avoided.
- Biometric data are privacy data and require a minimum level of protection. Biometric information is inseparably linked to a person and its life, and with possible risks to be abused. A safe, rights-respecting use of biometrics requires collaboration of experts, practitioners and stakeholders with diverse backgrounds (such as technical, business, government, philosophy, gender experts, etc.).
- The right to privacy is a crucial safeguard for the ability of individuals to live freely, form opinions, express themselves without fear and fully develop their personality. Privacy protection is key for the most disadvantaged and vulnerable members of society who are at greater risk of discrimination. Privacy is essential to allow civil society to operate and meaningfully participate in public life.
- The continued push for meaningful access comes against the background of a new digital divide where protecting privacy comes at significant economic cost and can undermine people's ability to opt-out.
- "Smart City" services will increasingly shape urban governance and public policies. Insight is needed in the use and protection of personal data, and the existence of legal gaps that may unintentionally allow social and economic discrimination, including discrimination in access to public services.

Algorithms

- A better understanding of how algorithms affect people's lives, of the potential risks of automated or algorithmic decision making, and of their impact on human rights and the right to privacy, will allow adequate technical and policy solutions, including a right to explanation.

Internet of Things

- The Internet of Things is the key driver of the digital revolution and creates new opportunities for our society, such as new products and services, but also creates vulnerabilities. Cybersecurity is a basic requirement for trust in the Internet of Things, as vulnerabilities could undermine the trust of individual users, and of the society as a whole. A joint global or regional approach is also needed, as the Internet of Things is a cross-border phenomenon.

Hate Speech

- The distinction between hate speech and the freedom to express unpopular opinions can be complex. The removal of content raises important challenges and can't be the full answer to the problem. The challenges related to hate speech require a holistic approach. There's a need for stakeholder education and cooperation, the development of tools which empower citizens and new reporting systems.

Legal & Regulatory issues

- Businesses have to protect themselves against the exponentially increasing number and variety of threats in the digital environment, but also depend on governments for legal counter-offensive actions against attackers. Public policy should further evolve and clarify the conditions, limits, and safeguards for proactive defensive measures by the private sector.

- Cybersecurity norms could be viewed as an important mechanism for State and non-State actors to agree on a responsible way to behave in cyberspace, given that the speed of legislation often falls behind the pace of changes in the sphere of cybersecurity.
- Both social platform giants and governments increasingly recognize the need for regulation. It is important for enhanced cooperation in the regulatory process, along with a sufficient level of multistakeholder participation in order to regulations to be efficient and enforceable. Risk management measures should also be embedded in regulations. Regulatory public-private partnerships could become a solution for securing political buy-in and predictability for the States and for economic profitability for tech companies. A “take it or leave it” approach is not helpful, and therefore, more resources and efforts are needed for efficient modalities of joint regulatory process in moving forward.

Cybersecurity Best Practices

- The successful implementation of a collaborative model for cybersecurity strategy development and implementation resides in agile adaptability, transparency, and trusted information sharing among and between all participants. Cybersecurity collaborations should display both vertical and horizontal collaboration between stakeholders, be descriptive rather than prescriptive, and be sufficiently agile in order to adapt alongside evolving cyber risks and technologies. Participation should extend not only to public and private sector entities who tend to own and control critical information infrastructure, but also to stakeholders from other sectors (e.g., the banking and finance sectors, business process outsourcing (BPO), health, tourism, and energy sectors) and non-profit stakeholder groups (e.g., the technical community, academia, and civil society).
- Private-public partnerships (PPPs) in cybersecurity should allow the government and major Internet service providers (ISPs) to pool their resources and know-how to tackle key aspects of cybersecurity, including protection of critical infrastructure and the fight against cybercrime. The effective cooperation between public and private actors countering cybercrimes is often challenged by obligations regarding disclosure and exposure; evolving liability and regulatory landscapes; cross-border data transfer restrictions and investigations of cybercrime.
- It is important that countries implement national cybersecurity measures through a risk-based approach. Cybersecurity policymaking must take into account the social and economic opportunities offered by the digital environment, while also guaranteeing fundamental rights. A dynamic balance between cybersecurity, economic development and human rights requires answers that are not limited only to technical solutions strictly aimed at eliminating the threat. On the contrary, in order to reap the social and economic benefits of digitalization, while protecting fundamental values, stakeholders must reduce risk to an acceptable level.
- Stakeholders should promote enhanced coordination and collaborative, risk-based frameworks of regional and national cybersecurity initiatives. A more meaningful global-oriented approach and more strategic risk-based collaboration in building national and regional cybersecurity capacity will enable nimble responses to security challenges.
- Threats to cybersecurity impact governments, private companies and people in general. Norms are helpful in general, on different aspects and from various parts of the world, but more efforts are needed to involve non-State stakeholders in the development and implementation of norms.

**This is a preliminary draft version of IGF Messages open to community inputs. To provide feedback on the Messages, please write to igf@un.org.*