IGF Internet Governance Forum

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

IGF 2018 Messages - Cybersecurity, Trust and Privacy

Overarching message

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 became 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 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.
- 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, being identified as the window or risk or threat when in the first place, cybersecurity measures should protect 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, information sharing and 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, 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 also be respected as basic principles in Internet governance. On top of that specific answers should be developed for implementation 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.
- Appropriate requirements and necessary legal, procedural and institutional safeguards for human rights with respect to the use of biometric information, including the architecture of biometric systems, should allow a maximal use of the opportunities provided by reliable technologies while avoiding and mitigating their risks and adverse impacts (such as the risk of identity theft, or the unlawful tracking and monitoring of individuals).
- The right to privacy is a crucial safeguard for the ability of individuals to live freely, to form opinions, to express themselves without fear and to fully develop their personality. Privacy protection is key for the most disadvantaged and vulnerable members of society who are at greater risk of discrimination, and privacy is an essential condition 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.
- Given the role that "Smart City" services are likely to play in shaping urban governance and public policies, and their impact on city dwellers, there is a pressing need to scrutinise the regulatory and governance dimensions of Smart Cities. This relates particularly to the use and protection of personal data, and to identifying legal gaps that may unintentionally allow social and economic discrimination, with particular regard to the access to public services. It is urgent to obtain insight into the nature and production of urban big data, the composition and functioning of urban analytics and control centres related to smart cities, and the privacy and security implications of the adopted forms of governance for citizens on a global scale.

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 share unpopular opinions has the potential to be complex, in some cases. The removal of content raises important challenges and can't be the full answer to the problem. 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 Best Practices

Collaboration

- 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 participations. 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 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 when solving security problems, 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.

**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.*