IGF Internet Governance Forum

IGF BERLIN 2019

Messages from IGF 2019

Child safety
Fake news

Deep fakes
Cyber attacks
Domain Name System

Security, Safety, Stability and Resilience

Hate speech
Encryption

Trust
Cybercrime
Internet Protocols
Freedom of expression

Table of Contents

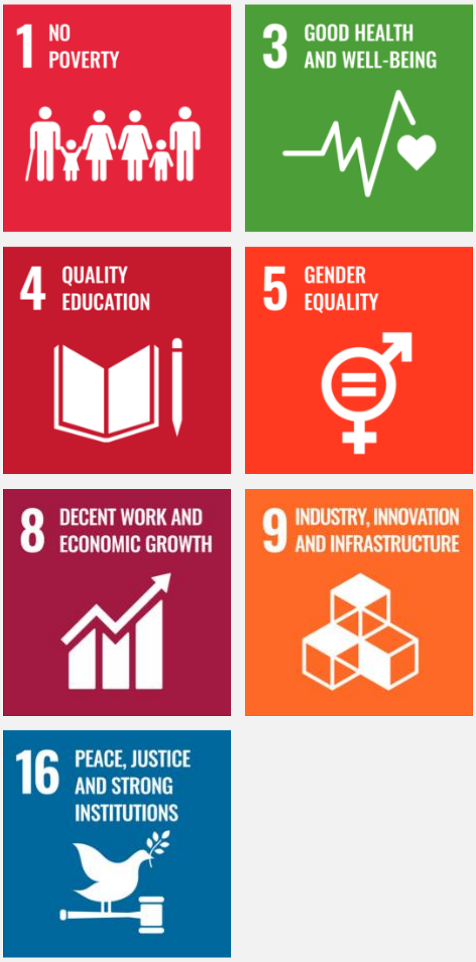
Introduction: Security, Safety, Stability and Resilience

About the Theme

At IGF 2019, discussions 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 of cybersecurity, 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.

Related Sustainable Development Goals (SDGs)


1 NO POVERTY
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
16 PEACE, JUSTICE AND STRONG INSTITUTIONS

Issues Associated with Security, Safety, Stability and Resilience

- Child Online Safety
- Child Sexual Abuse Material (CSAM)
- Cyber Attacks
- Domain Name System
- Internet Protocols
- Trust and Accountability
- Internet Resources
- Cyber Crime
- Encryption
- Fake News
- Freedom of Expression Online
- Deep Fake Videos
- Hate Speech

How the Berlin Messages on Security, Safety, Stability and Resilience were Developed

The Berlin messages provide policy makers with a quick, high-level overview of policy trends in the Internet space for 2019. The first set of high-level IGF messages were compiled during IGF 2017. They were well-received by forum participants, so have been continued at subsequent IGFs.

The Berlin messages were compiled and updated throughout the week of IGF 2019. On the mornings of IGF 2019 Days 3 and 4 of, three living documents, containing cumulative thematic messages drawn from the forum's discussions, were published on the IGF website for the consideration and input of participants.

https://www.intgovforum.org/multilingual/content/berlin-igf-messages

The final set of messages on security, safety, stability and resilience are contained in the following pages.

Did You Know?

A New Framework for Organizing Discussions Introduced at IGF 2019

In a new approach to shaping the programme in 2019, the MAG used the submissions received in response to the annual public call for issues to develop a more thematic, focused and non-duplicative design of the schedule. The three main themes that emerged out of this process helped shape many of the preparatory and intersessional work processes for IGF 2019:

- *Data governance*
- *Digital inclusion*
- *Security, safety, stability and resilience*

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.
- 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 remove or block illegal content, should also reach out to and cooperate with law enforcement agencies to provide information for preventive measures.
- When online platform operators remove harmful and illegal content, it would be useful to preserve the material as evidence, to support law enforcement investigation and criminal prosecution.
- Policy makers and responsible parties can gain more insight into the possibilities and limitations of technical measures and solutions through collaborative multistakeholder partnerships.

Security and Resilience of the Infrastructure

- Without an understanding of how the internet really works, measures to defend the network risk to break what they want to protect. As the technology continues to evolve over layers and layers of Internet infrastructure, concepts as basic as interoperability and peering are of absolute importance for a robust network development.
- 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, into effective and predictable policy implementation, it would be useful to standardize definitions and terms.
- Developing deeper understandings of the different roles that different stakeholders can take in discussions and the identification of possible solutions could led to more practical outcomes for all.
- To ensure that stakeholders with limited resources – particularly civil society – can engage and contribute meaningfully to policy discussions, it is important not to create multiple parallel discussions on the same issues.
- 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.

Best Practice Forum on Cybersecurity

In addition to community-proposed sessions that were explicitly included under the work track of Security, Safety, Stability and Resilience, IGF 2019’s intersessional activities included a Best Practice Forum (BPF) on Cybersecurity:

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

Outcome document, *Cybersecurity Agreements*:

https://www.intgovforum.org/multilingual/filedepot_download/8395/1896

The work of the BPF was presented to the intersessional consultative meeting of the United Nations Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security in December 2019. A number of participants at the meeting mentioned the BPF as an example of how multistakeholder dialogue is of value to helping a peaceful and stable cyberspace.

https://www.intgovforum.org/multilingual/content/igf-2019-bpf-on-cybersecurity-contributes-to-un-oewg

Previous Discussions on Security, Safety, Stability and Resilience at IGF

Security, safety, stability and resilience have been discussed at IGF in various forms dating back to 2005, where the "Security" was one of the original main themes of IGF.
Below is a summary of more recent discussions, since IGF's mandate was renewed by the United Nations General Assembly at the end of 2015.

Digital inclusion issues were raised in a number of different contexts in the previous three IGFs:

IGF 2016 Jalisco, Mexico

Main sessions:

- Assessing the Role of Internet Governance in the Sustainable Development Goals (SDGs)
- Sustainable Development, Internet and Inclusive Growth
- Connecting Human Rights: Emphasizing Economic, Social and Cultural Rights on the Internet

Intersessional work programs:

- Policy Options for Connecting the Next Billion(s)
- BPF on Gender and Access
- BPF on Internet Exchange Points

Workshop tracks on:

- Cybersecurity
- Critical Internet resources

IGF 2017, Geneva, Switzerland

Main sessions:

- Empowering Global Cooperation on Cybersecurity for Sustainable Development & Peace'
- 'Local Interventions, Global Impacts: How Can International, Multistakeholder Cooperation Address Internet Shutdowns, Encryption and Data Flows'

Intersessional work program:

- BPF on Cybersecurity

Cybersecurity was also the most popular thematic tag chosen by workshop organizers.

Messages related to security, safety, stability and resilience are contained in the Chair's Summary of IGF 2017:

- https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4223/919

IGF 2018, Paris, France

Security, Safety, Stability were at the core of the IGF in Paris, where the main theme of the event was "The Internet of Trust".

Main session:

- Cybersecurity, trust and privacy

Intersessional work program:

- BPF on Cybersecurity

Workshops categorized under the following two themes:

- Cybersecurity, trust and privacy
- Security, safety, stability and resilience

IGF 2018 produced the following messages related to security, safety, stability and resilience:

- Cybersecurity, Trust & Privacy
  https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6037/1408

Annex A: Development of the IGF 2019 Track on Security, Safety, Stability and Resilience

In the March 2019 calls for workshop proposals, open forums, Dynamic Coalition and National, Regional and Youth IGF collaborative sessions, organizers were invited to identify under which main theme their sessions would fall. Members of the Multistakeholder Advisory Group (MAG) put together the following information to assist IGF participants frame their sessions according to the main themes:

https://www.intgovforum.org/multilingual/content/igf-2019-themes

Workshop proposers were also given the option of selecting from a range of more specific associated issues/tags. In the leadup to the meeting in Berlin, each of the sessions associated with the main themes was coordinated by a small set of volunteers from the Multistakeholder Advisory Group (MAG).

How the Discussions on Security, Safety, Stability and Resilience Track Were Coordinated at IGF 2019

There was an introductory session to set the scene for the discussions throughout the week:

https://www.intgovforum.org/multilingual/content/introductory-breakout-session%C2%A0security-safety-stability-resilience

On Day 4, there was a concluding breakout session to reflect on the discussions that had been held throughout the week:

https://www.intgovforum.org/multilingual/content/concluding-breakout-session%C2%A0security-safety-stability-resilience

A brief summary of the reports presented during the concluding breakout session was included in the "Bringing It All Together" session on the afternoon of Day 4:

https://igf2019.sched.com/event/SU6X/bringing-it-all-together

List of Sessions

In total, there were 32 sessions on the theme of Security, Safety, Stability and Resilience at IGF 2019.

Dynamic Coalition (DC) sessions	
Data Governance on the Internet Space, by the Internet Model (DC on Core Internet Values and DC on IoT)	https://www.intgovforum.org/multilingual/content/igf-2019-data-governance-on-the-internet-space-by-the-internet-model
How to Balance Children's Right to Play and to be Protected (DC on Child Online Safety)	https://www.intgovforum.org/multilingual/content/igf-2019-how-to-balance-childrens-right-to-play-and-to-be-protected
National and Regional and Youth IGF (NRI) sessions	
Collaborative Session on Cybersecurity	https://www.intgovforum.org/multilingual/content/nris-collaborative-session-on-cybersecurity-0

Collaborative Session on Harmful Content Online	https://www.intgovforum.org/multilingual/content/nris-collaborative-session-on-harmful-content-online-0
Collaborative Session on Privacy Online	https://www.intgovforum.org/multilingual/content/nris-collaborative-session-on-privacy-online-0
Open Forums	
Collaborative Multistakeholder Approaches in Cybersecurity (Commonwealth Telecommunications Organisation)	https://www.intgovforum.org/multilingual/content/igf-2019-of-16-collaborative-multistakeholder-approaches-in-cybersecurity
Disinformation Online: Reducing Harm, Protecting Rights (Department for Digital, Culture, Media and Sport, UK Government, and Atlantic Council's Digital Forensic Research Lab)	https://www.intgovforum.org/multilingual/content/igf-2019-of-44-disinformation-online-reducing-harm-protecting-rights
DNS, Threats and Opportunities (ICANN)	https://www.intgovforum.org/multilingual/content/igf-2019-of-6-icann-dns-threats-and-opportunities
Exceptional Access and the Future of the Internet Security (Internet Society)	https://www.intgovforum.org/multilingual/content/igf-2019-of-38-exceptional-access-and-the-future-of-the-internet-security
Human Rights and Digital Platforms – Contradiction in Terms? (Council of Europe)	https://www.intgovforum.org/multilingual/content/igf-2019-of-19-human-rights-and-digital-platforms-%E2%80%93-contradiction-in-terms
Information Sharing 2.0: Privacy and Cybersecurity (Israel National Cyber Directorate)	https://www.intgovforum.org/multilingual/content/igf-2019-of-45-information-sharing-20-privacy-and-cybersecurity
Online Protection of Underage Users (Cyberspace Administration of China)	https://www.intgovforum.org/multilingual/content/igf-2019-of-14-online-protection-of-underage-users
Trust, Norms and Freedom in Cyberspace (Estonian Ministry of Foreign Affairs)	https://www.intgovforum.org/multilingual/content/igf-2019-of-22-trust-norms-and-freedom-in-cyberspace
Workshops	
Cybersecurity Concerns Everyone - Responsibility and Education Throughout the Digital Supply Chain	https://www.intgovforum.org/multilingual/content/igf-2019-ws-195-cybersecurity-concerns-everyone-responsibility-and-education-throughout-the
Digital Sovereignty and Internet Fragmentation	https://www.intgovforum.org/multilingual/content/igf-2019-ws-59-digital-sovereignty-and-internet-fragmentation
How and Why to Involve Perspectives of Children Effectively	https://www.intgovforum.org/multilingual/content/igf-2019-ws-23-how-and-why-to-involve-perspectives-of-children-effectively
Internet de-tox: A Fail-Proof Regimen to End Online Sexism	https://www.intgovforum.org/multilingual/content/igf-2019-ws-247-internet-de-tox-a-fail-proof-regimen-to-end-online-sexism
IPv6 Independence Day: Rest in peace IPv4	https://www.intgovforum.org/multilingual/content/igf-2019-ws-403-ipv6-independence-day-rest-in-peace-ipv4
Kids online: what we know and can do to keep them safe	https://www.intgovforum.org/multilingual/content/igf-2019-ws-137-kids-online-what-we-know-and-can-do-to-keep-them-safe

Misinformation, Responsibilities & Trust	https://www.intgovforum.org/multilingual/content/igf-2019-ws-85-ws-268-misinformation-responsibilities-trust-%E2%80%8E
Public Diplomacy v. Disinformation: Are There Red Lines?	https://www.intgovforum.org/multilingual/content/igf-2019-ws-295-public-diplomacy-v-disinformation-are-there-red-lines
Public Health Online: Shadow Regulation-Access to Medicines	https://www.intgovforum.org/multilingual/content/igf-2019-ws-92-public-health-online-shadow-regulation-access-to-medicines
Quantifying Peace and Conflict in Cyberspace	https://www.intgovforum.org/multilingual/content/igf-2019-ws-131-quantifying-peace-and-conflict-in-cyberspace
Roadmap for Confidence Building Measures (CBM) in Cyberspace	https://www.intgovforum.org/multilingual/content/igf-2019-ws-341-roadmap-for-confidence-building-measures-cbm-in-cyberspace
Should We Tackle Illicit Content Through the DNS?	https://www.intgovforum.org/multilingual/content/igf-2019-ws-331-should-we-tackle-illicit-content-through-the-dns
Tackling Cyberbullying on Children with Digital Literacy	https://www.intgovforum.org/multilingual/content/igf-2019-ws-95-tackling-cyberbullying-on-children-with-digital-literacy
Tackling Hate Speech: A Multi-Stakeholder Responsibility	https://www.intgovforum.org/multilingual/content/igf-2019-ws-150-tackling-hate-speech-a-multi-stakeholder-responsibility
Tackling Hate Speech Online: Ensuring Human Rights For All	https://www.intgovforum.org/multilingual/content/igf-2019-ws-177-tackling-hate-speech-online-ensuring-human-rights-for-all
Tech Nationalism: 5G, Cybersecurity and Trade	https://www.intgovforum.org/multilingual/content/igf-2019-ws-41-tech-nationalism-5g-cybersecurity-and-trade
Towards a Human Rights-Centered Cybersecurity Training	https://www.intgovforum.org/multilingual/content/igf-2019-ws-159-towards-a-human-rights-centered-cybersecurity-training
Transparency and Control for the Internet of Things	https://www.intgovforum.org/multilingual/content/igf-2019-ws-307-transparency-and-control-for-the-internet-of-things
Usual Suspects: Questioning the Cybernorm-making Boundaries	https://www.intgovforum.org/multilingual/content/igf-2019-ws-63-usual-suspects-questioning-the-cybernorm-making-boundaries

Annex B: Illustrative Policy Questions Developed by the IGF MAG to Assist Participants Develop Session Proposals

Co-operation and collaboration in Cybersecurity / Response to Cyberattacks:

- How can cooperation and collaboration on national, regional and global levels help to increase cybersecurity?
- What should govern the response of different stakeholders to state-sponsored cyber attacks?
- What legal regulations are already in place but potentially need to be enforced and what new legal regulations should be created to address upcoming threats? What role do Internet protocols play in the fight against cyber attacks?
- What role can institutional arrangements such as CERTs etc. play?
- What role should different stakeholders play in cybersecurity capacity building approaches?

Regulatory and technical approaches for safety:

- How can risks of contact and content (including violence against women, children and all vulnerable groups be addressed successfully by legal and regulatory approaches as well as by technical instruments and how can digital civility be increased?
- How can children's rights to participation, access to information, and freedom of speech be preserved and balanced with their right to be protected from violence, exploitation and sexual abuse in the online environment?
- How can their resilience be increased by means of capacity building, media literacy, support and guidance in the digital environment?
- How can all forms of inappropriate sexualisation of childhood in digital areas be addressed by effective means?
- Which technical and regulatory instruments can reinforce the fight against CSAM?
- What are adequate techniques or technologies to fight all forms of online harassment including sexual harassment?

Trust and Accountability:

- How can trust and accountability be restored?
- What role should Internet platforms play in defining the standards for acceptable content in light of freedom of speech?
- How can globally accepted standards be developed?
- What kind of collaboration could be created among Internet platforms and media outlets to fight disinformation and fake news?
- Where is the middle ground between increasing demands for proactive content policing by digital platforms and the necessary neutrality and legal certainty for platforms?

Safety, data protection, and consumer rights:

- 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?
- How can consumer rights and their capacity to protect themselves and their data be reinforced?