Human Rights Impact of Cybersecurity Laws, Practices and Policies

Contribution of the Freedom Online Coalition

Cybersecurity is not just about the security of assets and information. Cyberattacks have also imperilled individuals' safety, both because some cybersecurity laws have suppressed human rights and fundamental freedoms, and because malicious actors have undermined individuals' safety online. Individual security,– whether offline or online, – should be a core purpose of cybersecurity; a secure Internet is central to the respect for human rights in the digital context. Cybersecurity measures should reinforce the availability, integrity, and confidentiality of information. These are essential to the security of the individual, especially in the digital context where physical security and digital information can be linked. Individuals cannot exercise their human rights if they do not have the security to do so. It therefore follows that cybersecurity and human rights are complementary, mutually reinforcing, and interdependent.

As such, in 2016, the Freedom Online Coalition adopted a statement[1] on a human rights based approach to cybersecurity, which affirms that human rights and cybersecurity are complementary, interdependent and mutually reinforcing, and that cybersecurity policies and practices should be rights respecting by design. Additionally, the Tallinn Agenda affirmed that human rights and fundamental freedoms and security online are complementary concepts. These documents highlighted that framing human rights as antithetical to cybersecurity is not only misleading, but undermines public safety and security, as well as freedom. Both human rights and cyber security need to be pursued together to effectively promote freedom and security: without either one, overall security, – offline and online, – is compromised.

Since 2016, new cybersecurity challenges have emerged. In response, numerous new national policies, laws and practices have been developed and adopted. Nevertheless, the FOC recommendations on human rights and cybersecurity remain relevant, particularly given the continued focus on cybersecurity in the UN and elsewhere.

The purpose of this statement is to reaffirm and build on the 2016 commitments while elaborating further on the human rights based approach to cybersecurity as a basis for strengthening cybersecurity, promoting stability in cyberspace,[2] and promoting emerging technologies that are

[1] https://freeandsecure.online/resources/foc-statement-support-cybersecurity-human-rights-recommendations/ - This statement endorses the work of the FOC Working Group 1 on an Internet Free and Secure, Details on the WG can be found here: https://freedomonlinecoalition.com/working-groups/working-group-1/

[2] For example, as noted by the Global Commission on the Stability of Cyberspace (GCSC), stability of cyberspace is the condition where individuals and institutions can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services in cyberspace is generally assured, where change is

trust-worthy whilst ensuring the protection of all online users. The statement contains recommendations for national cybersecurity practices and international cybersecurity processes and is based on recommendations developed by the multistakeholder FOC working group.

As we all have a stake in an open, free, secure, interoperable and reliable cyberspace, it is critical that the human dimension of cybersecurity is incorporated in cyber policies and practices.

International efforts to promote stability in cyberspace

While acknowledging that governments play a primary role in developing domestic cybersecurity measures, we consider the incorporation of perspectives from all relevant and affected stakeholders at the earliest stage of cyber security policy development to be critical to ensuring a holistic consideration of the implications of cybersecurity measures for human rights.

At the international level, the role of intergovernmental organisations, such as the United Nations, are becoming increasingly relevant in convening discussions about responsible State behaviour in cyberspace through the United Nations Group of Governmental Experts (UNGGE) on Advancing responsible State behaviour in cyberspace in the context of international security and the United Nations Open-ended Working Group (OEWG) on Developments in the field of information and telecommunications in the context of international security. Significant work is also conducted at regional levels by organisations including the African Union (AU), the European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), Council of Europe (CoE) and the Regional Forum of the Association of Southeast Asian Nations (ARF).

Promoting stability of cyberspace is not the responsibility of States alone. A number of multistakeholder initiatives recognise the important role of other actors including industry, civil society, the technical community and academia. The private sector also plays a critical role in creating and maintaining digital services and infrastructure as well as introducing innovative initiatives promoting cybersecurity leadership.

Cybersecurity challenges

The rapid increase, persistence and relentlessness of malicious cyber activities against governments, the private sector and civil society is driving a sense of urgency. These activities have led to large-scale data breaches and exploitation of the vulnerabilities of digital economies.

---

managed in relative peace, and where tensions are resolved in a peaceful manner..
https://cyberstability.org/news/request-for-consultation-definition-of-stability-of-cyberspace/

Cybersecurity threats have the potential to affect ICT infrastructure worldwide by impacting physical infrastructure, software and hardware, as well as systems upon which our societies, communities, and individuals depend. As the world becomes increasingly dependent on digital technology, malicious actors exploiting cybersecurity vulnerabilities will continue to imperil the lives, the health and well-being of people everywhere.

While State authorities are responsible for protecting the human rights of those in their territory and law enforcement should be enabled to assist victims of harmful cyber activities, the FOC is deeply concerned about the practices by some States of asserting excessive control over the Internet under the pretence of ensuring national security while disregarding international human rights law and the principles of an open, free, secure, interoperable and reliable Internet. In particular, the FOC is alarmed at the growing number of restrictions placed on the exercise of the right to freedom of opinion and expression online, including where States have manipulated or suppressed online expression in violation of international law, including through discriminatory or politically motivated Internet censorship or Internet shutdowns, unlawful or arbitrary monitoring, and the arrest and intimidation of online activists for exercising their human rights.

Additionally, some technologies and practices pose risks to the enjoyment of human rights when used for unlawful or arbitrary surveillance, whether mass or targeted, including through the use of facial recognition or other biometric technologies; unlawful or arbitrary restrictions on encryption and anonymity; unlawful restrictions of content; and, network shutdowns that are inconsistent with international human rights law. The FOC also acknowledges that the risks that some technologies and practices pose to the enjoyment of human rights can be exacerbated when governments seek to compel the suppliers of such technologies to cooperate with their security and intelligence agencies without any democratic or independent checks or balances on these authorities. This capability threatens the principles of an open, free, secure, interoperable and reliable Internet, and the rule of law. The FOC also notes the challenges posed to business and government alike by the scarcity of domestic laws, international best practice, and private sector awareness of human rights abuses linked to the export of items with surveillance capabilities and tools to support efforts to conduct human rights due diligence to mitigate the risk of potential adverse human rights impacts.

Recommendations to States

FOC affirms the recommendations of the FOC working group on human rights based approaches to cybersecurity (https://freeandsecure.online/recommendations/) and the Tallinn Agenda, which confirmed that the same rights that people have offline must also be protected online and that respect for human rights and security online should be treated as complementary concepts, and recommends the following:

- States need to comply with their obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation.

- States need to develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to minimise potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists. This includes building, where appropriate, supporting processes and frameworks for transparency, accountability, judicial or other forms of independent and effective oversight, and redress towards building trust. It may also include embedding the principles of legitimacy, legality, necessity or proportionality into policy and practice.
- Cybersecurity-related laws, policies, and practices should be developed through ongoing open, inclusive, and transparent approaches that involve all stakeholders.
- States should promote international cooperation on cyber issues that focuses on protecting and upholding human rights in order to build mutual trust between all stakeholders.
- States should seek to implement the rules, norms and principles of responsible State behaviour contained in the (2010, 2013, 2015) consensus reports of the UNGGE.
- States should find ways to draw attention to acts contrary to these rules, norms and principles of responsible State behaviour in order to increase accountability, transparency and help build patterns of responsible behaviour.
- As humans are directly impacted by potential threats in cyberspace, including cyberattacks, due attention should be paid to the human dimension of cybersecurity. This includes direct and indirect harm to individual well-being manifesting itself in a range of ways including loss of life, loss of access to vital services, financial loss, undermining of democratic institutions and processes, suppression of the rights to freedom of expression and freedom of association, and failure to respect the right to be free from arbitrary or unlawful interference with privacy, etc.
- In compliance with best practice data protection laws and regulations, States should consider, as appropriate, collecting and sharing data, as well as funding research, on the nature and scale of these aforementioned harms, to underpin and drive a human-focused international cybersecurity capacity building agenda.
- States should encourage education, digital literacy, critical thinking, information exchange and technical and legal training as a means to improve cybersecurity and build collective capacity at local, regional, and global levels.
- States should encourage private sector actors to adhere to the UN Guiding Principles on Business and Human Rights, to improve their accountability and to share best practices in this respect and help to share lessons learned.
- States should encourage private sector actors to promote and practice good cyber hygiene.

We as the Freedom Online Coalition members intend to lead by example and therefore commit to the above recommendations. We encourage all States to implement these recommendations when discussing, developing and implementing cybersecurity related policies.