# An Internet free & secure: a human rights based approach to cybersecurity

INTERNET FREE & SECURE INITIATIVE

# Contents

# 01 Introduction

*The Freedom Online Coalition (FOC) is a group of  30 governments that works to support Internet freedom and protect fundamental human rights worldwide. From 2014 – 2017 the coalition supported a Working Group, “An Internet Free and Secure”,*[1] *comprised of experts from the private sector and civil society in partnership with member states to bring a human rights framing to ongoing debates on cybersecurity. With cybersecurity a critical issue on the international agenda, there was a recognition of the need for an informed debate on the relationship between governance, security, and fundamental rights and freedoms online, involving all stakeholders.*

*The following definition of cybersecurity and recommendations on cybersecurity and human rights are the product of the Working Group.*

In 2016, the FOC issued a statement supporting the Working Group’s output, encouraging:

> “all stakeholders involved in cybersecurity-related activities to take into account the Working Group’s Definition and Recommendations in their policy development and deliberations.”

Why do we need a human rights based approach to cybersecurity policy-making? In the public debate about how to provide security in the digital context, the dominant narrative has become increasingly entrenched pitting privacy and other human rights against public safety and national security. In practice, though, threats to privacy and other human rights can also harm public safety and security. This

**Notes**

[1] https://freedomonlinecoalition.com/working-groups/working-group-1/blog8/

binary framing is therefore damaging to both sides of the equation, and creates antagonisms where mutual reinforcement is possible. Framing privacy and other human rights as antithetical to public safety and national security is not only misleading, but undermines public safety and security, as well as freedom. Raising the profile of human rights protections in existing cybersecurity policy-making is necessary to offset this trend.

In the context of increasing cyber vulnerability, where cybersecurity and cybercrime challenges are increasing in frequency and complexity, there is a need for all stakeholders to work together to preserve human rights, particularly privacy and free expression. Individual security is a core purpose of cybersecurity and a secure Internet is central to human rights protection in the digital context. Any definition of cybersecurity must therefore reinforce that privacy and confidentiality of information are essential to the security of people, as well as to data, especially in the digital context where physical security and digital information are linked.

Cybersecurity and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security. Recognizing that individual security is at the core of cybersecurity means that protection for human rights should be at the center of cybersecurity policy development. Such an approach is instrumental in reminding policy-makers that cybersecurity must take into account individual security and human rights and that, as a consequence, cybersecurity policies should be human rights respecting by design.

The primary task of the FOC Working Group was to help bring a paradigm shift to cybersecurity so that human rights and cybersecurity are understood to be interdependent and mutually reinforcing. The challenge facing the Working Group was how to translate this paradigm shift into action across a diversity of policy spaces and change the conversation on cybersecurity by defining individual security and human rights as the starting point. Doing so requires breaking down policy-silo boundaries, dislodging the dominant rights-versus-security paradigm, and building evidence that human rights and cybersecurity are mutually reinforcing and interdependent.

To that end, the FOC Working Group developed a new definition for cybersecurity and a set of cybersecurity and human rights focused policy recommendations that can be applied in a variety of situations. The definiton and recommendations build upon and advance existing cybersecurity policy-making efforts while prioritising human rights. They offer guidance to all stakeholders involved in cybersecurity matters, and in particular those involved in developing and implementing cybersecurity policies and frameworks.

# 02 Definition

The term “cybersecurity” is used by different stakeholders to reference many different subjects often depending upon context, ranging from national security, to data security, to critical infrastructure security, and beyond. While it is true that numerous definitions relating to cybersecurity exist, it is difficult to find any cybersecurity definitions that include clear commitments to and respect for human rights. Accordingly, the FOC Working Group believed it crucial to put forth a human rights-respecting cybersecurity definition that others could adopt and integrate into policies and publications.

The definition encompasses the belief that respecting human rights should be a central part of cybersecurity-related decision making. Raising the profile of human rights protections in existing cybersecurity policy-making is necessary to offset the current trend of addressing cybersecurity through the lens of national and international security and to remind policy makers that cybersecurity must take into account security for individuals. In short, the definition reflects a framing of cybersecurity that shifts the perspective from a systems approach towards an approach that recognizes individual security as a core component of cybersecurity.

## Preamble

International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights.

## Definition

Cybersecurity is the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline.

**The definition includes three core elements:**

1. The ultimate goal of cybersecurity: **"to enhance the security of persons both online and offline**";
2. Articulation of how this ultimate goal and the dimensions of cybersecurity translate into technical terms: **"cybersecurity is the preservation…of the availability, confidentiality and integrity of information and its underlying infrastructure**"
3. The means through which this goal is being achieved: **"through policy, technology, and education**" with the understanding that "**policy**" includes the law.

The definition[2] supports the view that security and freedom (as well as cybersecurity and human rights) are deeply interrelated and synergistic, rather than zero-sum, and that cybersecurity and human rights protection are mutually reinforcing, interdependent, and both essential to promoting freedom and security.

**Notes**

[2] The Working Group's human rights and individual security focused definition of cybersecurity can be found here: https:// freeandsecure.online/definition/

*As defined by ISO 27000 standard which informed this process to ensure that the work of the technical community was adequately taken into account.

# 03

# Recommendations for human rights based approaches to cybersecurity

The following recommendations developed by the FOC Working Group “An Internet Free and Secure” bring a human rights framing to ongoing debates on cybersecurity and to encourage meaningful multistakeholder outputs that enhance and feed into existing cybersecurity processes.

These recommendations[3] are a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – effectively, that cybersecurity policies and practices are rights-respecting by design. The recommendations build on the above definition of cybersecurity and on existing frameworks, recommendations, and commitments to human rights in cybersecurity.

As noted above the Freedom Online Coalition commended these recommendations to all stakeholders – governments, international organisations, the private sector and civil society, including academic and technical communities – involved in cybersecurity policy development and implementation.

**Notes**

[3] The “Recommendations for Human Rights Based Approaches to Cybersecurity” can be found here: https://freeandsecure.online/ / recommendations/

## Recommendations

1. Cybersecurity policies and decision-making processes should protect and respect human rights.

2. The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.

3. Cybersecurity-related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk.

4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law.

5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.

6. Responses to cyber incidents should not violate human rights.

7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.

8. Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.

9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.

10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.

11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.

12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders

13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity.

Concerns related to specific practices – including surveillance and content control – are addressed in these recommendations in two ways. First, to the extent that cybersecurity is used to advance other unrelated objectives such as censorship or surveillance activities, Recommendation 5 specifically highlights that cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights. Moreover, with regard to content control and surveillance activities relating to cybersecurity, Recommendations 1 and 2 highlight that cybersecurity laws, policies, practices, and decision-making processes should protect and respect human rights.

# 04

# Statement of support by the 30 Governments of the Freedom Online Coalition

In October 2016, the Freedom Online Coalition issued the following statement:

"The Freedom Online Coalition recognises that as the world has become increasingly interconnected through information and communications technologies (ICTs), cybersecurity has become a critical issue on the international agenda. Cybersecurity threats are increasing in frequency and sophistication, asking for innovative solutions. This creates a growing need for all stakeholders to work together to address these issues in a manner that promotes and respects human rights.

Regrettably, the prevalent worldview is to see human rights and cybersecurity interests in absolute terms – one must be traded-off in the favor of the other. The Freedom Online Coalition maintains that human rights and cybersecurity are complementary, mutually reinforcing and interdependent. Both are essential for the promotion of freedom and security. The Coalition believes there is a pressing need to move beyond the dominant rights versus cybersecurity paradigm, by recognising that individual security is a core component of cybersecurity and a that secure Internet is central to promoting human rights.

The Freedom Online Coalition Working Group "An Internet Free and Secure", comprised of experts from the private sector, academia, civil society and select member states, is helping bring about this paradigm shift and translating it into action. It is seeking to increase the priority policy makers, private firms and other stakeholders place on individual security and human rights. … The Working Group has drafted a set of Recommendations for Human-Rights Based Approaches to Cybersecurity, which … can help to advance existing cybersecurity policy-making efforts while prioritising, promoting, and respecting human rights.

These Recommendations should not be read as creating new international law obligations, or as limiting or undermining any legal obligations a State may have undertaken or be subject to under international law with regard to human rights. The Freedom Online Coalition reaffirms that States must respect their international human rights obligations, including when implementing laws internally.

The Freedom Online Coalition applauds the direction of the work undertaken by Working Group 1, and hopes that this will work towards the realisation of a paradigm shift in cybersecurity policy making that is human rights respecting by design. We encourage all stakeholders involved in cybersecurity-related activities to take into account the Working Group's Definition and Recommendations in their policy development and deliberations."

Read the full statement here: https://freeandsecure.online/resource/

INTERNET FREE & SECURE INITIATIVE

The Internet Free and Secure Initiative (IFSI) promotes and builds on the work of the "Internet Free and Secure" Working Group of the Freedom Online Coalition (FOC), a partnership of 30 governments that works to further Internet freedom across the globe. From 2014 to 2017, the FOC Working Group advanced the normative debate on cybersecurity through developing a set of recommendations and a definition that promote human rights respecting and multistakeholder approaches to cybersecurity. IFSI is led and supported by members of the original FOC Working Group.

For more information or to reach IFSI
please email: **info@freeandsecure.online**