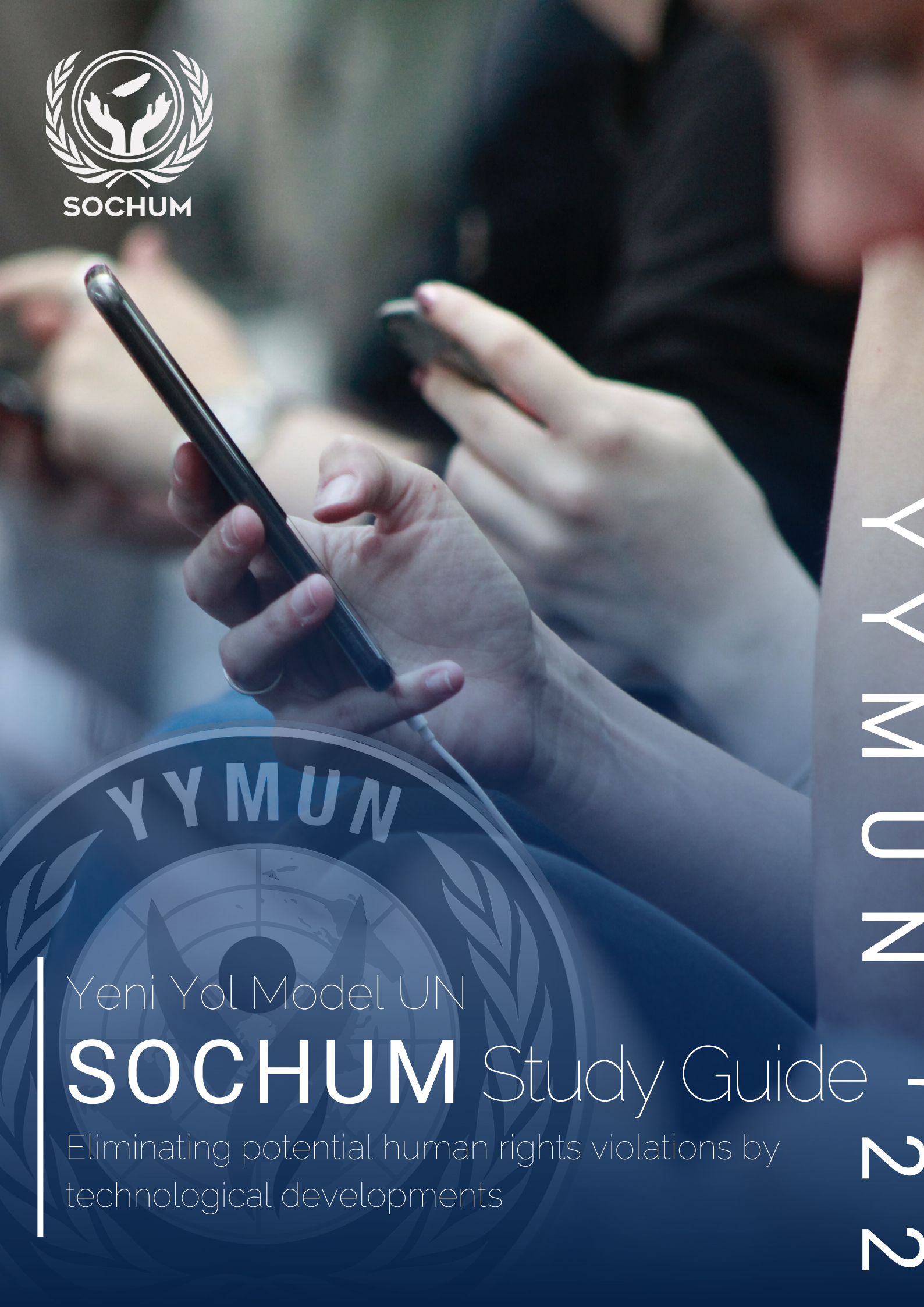

SOCHUM

YYMUN 2022

Yeni Yol Model UN

SOCHUM Study Guide

Eliminating potential human rights violations by technological developments

Table of Content

WELCOME LETTER FROM THE SGs

Dear delegates, advisors, parents, and future diplomats,

It is with utmost excitement that I welcome you to join us for the first-ever iteration of the Yeni Yol Model United Nations. I am honored to serve as the Secretary-General of a conference that embodies traditions of education and excellence, and I could not be more excited to host you at our conference. Over the three days of YY MUN, over 200 delegates from different cities and countries will discuss and solve pressing global issues, engage in diplomacy, and safely interact with their peers in the conditions of the pandemic.

I recommend that delegates with little experience with model United Nations simulations read the entire document carefully, as it will provide a thorough introduction to the dynamics of an actual committee session. Familiarity with the flow of the committee will allow a new delegate to jump into debate immediately upon arrival at the conference.

All the focal points of the committees have to be understood carefully. Please bear in mind that study
guides are not a comprehensive total review of the issue, and it merely serves as a path through which every delegate can start researching. The course of the committee will require agile reactions to every event, so it is in the best interest of every member of the committee if you were to complement this study guide with other resources and develop a comprehensive understanding of the issue.

It is my hope that the experiences had during our conference will inspire future
leadership, diplomacy, and knowledge that will stay with you for long after our gavel marks the end of
closing ceremonies.
On behalf of our entire Secretariat, welcome to Yeni Yol MUN.
Sincerely,

Dicle Naz Acu&Selin Aydın
Secretaries-General
Yeni Yol Model United Nations 2022

INTRODUCTION

General Look of the Committee:

The General Assembly is the main deliberative, policymaking, and representative organ of the United Nations. Comprising all 193 Member States of the UN, it provides a unique forum for multilateral discussion of international issues including peace and security.

The General Assembly exercises deliberative, supervisory, financial, and elective functions relating to any matter within the scope of the UN Charter. Its primary role, however, is to discuss issues and make recommendations, though it has no power to enforce its resolutions or compel state action.

The United Nations General Assembly Third Committee (SOCHUM) is one of six main committees at the General Assembly of the United Nations. It deals with human rights, humanitarian affairs, and social matters.

In this session of YYMUN, the SOCHUM committee will be discussing the ways of eliminating potential human rights violations by technological developments.

The Universal Declaration of Human Rights (UDHR)

The Universal Declaration of Human Rights (UDHR) is a watershed moment in human rights history. The Declaration was drafted by delegates from many parts of the world with various legal and cultural backgrounds, and it was declared by the United Nations General Assembly in Paris on 10 December 1948 as a shared standard of achievements for all peoples and nations. It establishes universal protection for fundamental human rights for the first time, and it has been translated into over 500 languages. The Universal Declaration of Human Rights is widely credited with inspiring and paving the way for the approval of more than seventy human rights treaties, which are now in force permanently at global and regional levels (all containing references to it in their preambles).

Whereas the acknowledgment of all members of the human family's inherent dignity and equal and inalienable rights is the cornerstone of world freedom, justice, and peace,

Whereas a world in which human beings enjoy the freedom of speech and belief, as well as freedom from fear and lack, has been declared as the highest ambition of the common people,

Whereas it is critical that human rights be preserved by the rule of law if a man is not forced to resort to rebellion against tyranny and oppression as a last resort,

While encouraging the establishment of cordial relations between states is critical,

Whereas the peoples of the United Nations have reaffirmed their faith in fundamental human rights, the dignity and worth of the human person, and equal rights for men and women in the Charter, and have resolved to achieve social progress and higher living conditions in greater freedom,

Whereas the Member States have committed to promoting universal respect for and observance of human rights and fundamental freedoms in collaboration with the United Nations,

While it is critical to have a common understanding of these rights and freedoms to fully realize this vow,

Consequently,

The General Assembly,

Proclaims this Universal Declaration of Human Rights as a common goal for all peoples and nations, with the goal that every individual and every organ of society, keeping this Declaration in mind, will strive to promote respect for these rights and freedoms through teaching and education, as well as through progressive national and international measures, to ensure their

universal and effective recognition and observance, both among the peoples of Member States and beyond.

One of the goals of the United Nations Charter is to maintain international peace and security. Violence and conflict impair long-term growth. Human rights abuses are the basis of conflict and instability, which always leads to further human rights violations. Actions to preserve and promote human rights have intrinsic preventative potential, while rights-based approaches to peace and security apply this power to efforts for long-term peace. The normative framework for human rights also offers a solid foundation for resolving major concerns inside or between countries that, if left unchecked, might lead to conflict. Human rights data and analysis is a tool for early warning and targeted action that has yet to be fully utilized.

Protection of Human Rights:

Second, since the formation of the UN more than 70 years ago, human rights principles have been understood to play an essential role in helping provide international peace and security. Human rights-respecting governments also have generally understood that respect for human rights and the rule of law reinforces their strength, rather than diminishing it. In our digitally interconnected and vulnerable context, where global and domestic terrorism is spreading, many governments have been tempted to utilize new digital technologies without regard for human rights, and without understanding the consequences of disregarding these values for security. As new technologies have emerged, public debate around how human rights are impacted has tended to be reactive, piecemeal, and often impractical. Given that so many dimensions of society have been disrupted by digital technology, it has been difficult for policymakers to see the bigger trends, understand the relationship between the parts, and assess top priorities. It's time for policymakers to be more proactive and holistic, and to advance practical solutions to priority global human rights challenges.

GENERAL OVERVIEW

As new technologies have become available, public discussion of how they affect human rights has tended to be reactive, fragmentary, and frequently unworkable. Given how digital technology has affected so many aspects of life, policymakers have struggled to recognize larger patterns, grasp the relationships between the pieces, and prioritize top objectives. It's past time for politicians to be more proactive and comprehensive in their approach to addressing numerous pressing global human rights issues.

As new technologies have become available, public discussion of how they affect human rights has tended to be reactive, fragmentary, and frequently unworkable. Given how digital technology has affected so many aspects of life, policymakers have struggled to recognize larger patterns, grasp the relationships between the pieces, and prioritize top objectives. It's past time for politicians to be more proactive and comprehensive in their approach to addressing numerous pressing global human rights issues.

These digital inequalities have the potential to worsen current global inequality and create situations that are more likely to lead to conflict. Almost all of the UN Sustainable Development Goals, which were established in September, rely on increasing global access to information and communication technology infrastructure. However, at this rate, meeting the UN objective of universal Internet access in underdeveloped countries by 2020 does not appear conceivable.

Even though the Internet may seem like an unuseful way to promote security for human rights, on the contrary Internet could be the perfect revolution for promoting human rights.
First of all, the biggest advantage of the Internet is that it enhances access to a larger audience. Nowadays, social media could be the best platform to share your ideas and promote the things you believe in. Technological advancements have empowered us to protect human rights by sharing our views with a larger audience. We can protect our rights by being aware of the best security practices and practicing them.

CURRENT ISSUES

Global Inequality:

One traditional human rights concern that has been aggravated by digital technology is **global inequality**. This is caused by the lack of access to technology, rather than the technology itself. While those of us who live in the digital ecosystem can't remember what daily life is like without Internet connectivity or our digital devices, the majority of people in the world have zero digital experience. Globally, nearly six out of ten people are not connected to the Internet. Even more stark is the fact that roughly 65 percent of people in the developing world do not yet use the Internet. And women generally have less access to the Internet (another expression of gender inequality), as do people living in rural areas.

These digital divides have the potential to significantly exacerbate existing global inequality and lead to conditions where conflict is more likely. Nearly all of the Sustainable Development Goals adopted in September depend on expanding access to information and communications technology infrastructure around the planet. Narrowing the digital divide must be ranked as a top human rights priority.

Violations in the name of "security":

Technology has exacerbated another problem from the pre-digital era: human rights violations committed in the name of national security and counterterrorism, even by democratic, human rights-respecting governments. New generations of digital technology have brought many significant changes to government capacities in law enforcement, counterterrorism, and foreign surveillance. The human rights implications of many of these new capacities were not fully appreciated before they were put to use. But security agencies around the world have been unwilling to rein in those new capacities, despite our deeper understanding of those implications.

Furthermore, in many countries facing terror threats, the imposition of vague and expansive cyber-related laws — without adequately considering or protecting human rights — has led to the erosion of some very basic human rights principles (e.g., that surveillance programs must be both necessary and proportionate). Ambiguous, imprecise, and unnecessarily intrusive counterterrorism laws have been replicated around the world by governments of all stripes. Even governments that see themselves as human rights champions have found it difficult to bring their counterterrorism activities under the rule of law.

For example, notwithstanding all the post-Snowden uproar in Europe about US mass surveillance, the French parliament adopted a "Law reinforcing measures relating to the fight against terrorism" in November 2014 that raises issues of compatibility with the rights to free movement, the presumption of innocence, and to free expression. The UK's Investigatory Power Bill, in its current form, would legalize mass global surveillance by UK security agencies, and allow extraterritorial hacking of computers, phones, and networks. And some members of the Freedom Online Coalition — a group of 29 governments convened for the specific purpose of reinforcing human rights protections online — continue to call for backdoors or exceptional access to encryption for themselves, without recognizing that such actions not only threaten the protection of human rights and privacy but also undermine their security.

PAST ACTIONS

By the Europen Council:

- The campaign was led by The Anti-Phishing Working Group (APWG) and the National Cyber Security Alliance (NCSA) to help users stay safer online. It includes customizable materials (posters, flyers, banners, etc.) that have been deployed by hundreds of enterprises and NGOs worldwide.
- Europol's cybercrime-prevention guides contain information that can help citizens protect themselves and their property.
- Europol's public campaign to help police officers trace the origin (location/country) of objects that appear in images with sexually explicit material involving minors and speed up investigations.
- No More Ransom (NMR) is an initiative by Europol's European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands' police, and McAfee to help victims of ransomware retrieve their encrypted data without having to pay the criminals.
- Better Internet for Kids (BIK) and the #SaferInternet4EU are EU Commission-funded initiatives aimed at creating a better Internet for Europe's children and youth. Safer Internet Centres have developed educational resources to help teachers, parents and children discover the online world safely.
- INHOPE is an active and collaborative global network of Hotlines, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet.
- "Through the Wild Web Woods" is an online game for teaching basic Internet safety in a fun and friendly fairy tale environment. The game is based on the Council of Europe's Internet Literacy Handbook.
- The UK Commonwealth Cyber Security Programme aims to deliver free, accessible, up-to-date, and comprehensive advice about staying safe online, to the people and businesses of the Caribbean.
- ChildSafeNet is raising awareness about protecting children and young people online.
- SWITCH's "Hack The Hacker" is a hands-on security awareness experience. In the style of an escape room, the participants have to solve puzzles in an analog game environment as a team.

- Cyber4Schools is an initiative of the Cyber Security Engagement Team For The East Midlands, in the UK. It contains resources for schools, students, and parents, as well as games and challenges with the aim of promoting a culture of cyber safety.

Other Actions Taken by the Governments:

Pakistan's *Prevention of Electronic Crimes Act*, as just one example, authorizes blocking websites deemed critical of officials and requires service providers to retain or provide authorities with access to copious amounts of people's data, which is open to abuse. Article 34 of Pakistan's Prevention of Electronic Crimes Act enables broad government powers of censorship, including authorizing blocking or removing online content if it considers it "necessary in the interest of the glory of Islam or the integrity, security or defense of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offense under this Act.

Other laws, like **Egypt**'s *Anti-Cyber And Information Technology Crimes Law*, have been used to prosecute people for using secure digital communications, which are crucial to keeping people safe online. For example, Article 15 presents A penalty of imprisonment for a period not less than 6 months and or a fine of no less than thirty thousand Egyptian pounds and no more than fifty thousand Egyptian pounds shall be inflicted on whoever accessed a site, private account or information system using authorized right of his own but exceeded the limits of this right in terms of time or access level.

Cambodia's proposed cybercrime law prohibits acts that vaguely constitute "disturbing, frightening, threatening, violating, persecuting or verbally abusing others by means of the computer." The United Arab Emirates' Federal Legal Decree No. 5/ 2012 on combating cybercrimes broadly criminalizes the use of information technology "with the intent of inciting to actions, or publishing or disseminating any information, news, caricatures, or other images liable to endanger state security and its higher interests or infringe on the public order."

In October 2020, **Nicaragua**'s Congress adopted a cybercrime law that criminalizes "publication" or "dissemination" of "false" or "distorted" information on the internet "likely to spread anxiety, anguish or fear." It also punishes anyone who publishes "false or distorted information" that "promotes hate and violence, [or] endangers economic stability, public order or health, or national security," terms that are not defined.

In March 2020, **Russia** introduced Article 207.1 into the criminal code for "public dissemination of knowingly false information in circumstances threatening the life and safety of citizens," punishable with up to three years of liberty restriction. A proposed cybercrime law in Eswatini outlaws publishing a statement or "fake news" through any medium, with the intention to deceive anyone else or any group of people.

Thailand's 2016 *Computer-Related Crime Act (CAA)* criminalizes publishing content that is "likely to cause damage to the public," including "false or partially false" data, "distorted or partially distorted" data, or data likely to "cause public panic" or harm "maintenance of national security, public safety, national economic security, public infrastructure serving the public interest." Rwanda's Law on Prevention and Punishment of Cyber Crimes prohibits the publication of "rumors."

POSSIBLE CONSIDERATIONS FOR THE FUTURE

Cyber resilience and digital security have become the heart of national security, international security, economic security, personal security, and human rights protection. The reliable functioning of critical Internet infrastructure is the backbone of the global economy, national security, as well as of human rights work. Protection of this critical infrastructure from hacking or attack is a shared priority for all of these actors and communities, as is digital security for users and their data. It is worth underscoring again that undermining digital security in the name of national security is nonsensical in the interconnected digital context.

Governments must embrace their obligation to provide security to citizens by strengthening the resilience of critical systems to withstand attack, as well as by shoring up capacities to thwart catastrophic cyber offensives in the first place. To the extent that the ability to thwart or withstand attack discourages future attacks, cyber resilience and digital security will enhance national security and strength on multiple levels.

To protect consumer interests, private sector actors need to embrace their responsibility to protect users' personal data as their first obligation. The trust of their users, as well as their economic bottom lines, will depend on it. Privacy and digital security are essential to the exercise of citizens' freedoms. Even more to the point, digital security is now intimately connected to the physical security of human rights defenders. And as connectivity expands in the efforts to overcome digital divides, basic digital hygiene and education must be packaged with connectivity by default for users globally.

BIBLIOGRAPHY

https://cybercrime-fr.org/wp-content/uploads/2020/04/Egyptian-cybercrime-law-.pdf

https://www.hrw.org/news/2016/03/25/digital-disruption-human-rights

https://www.hrw.org/