01

CYBERSECURITY AND HUMAN RIGHTS

CAROLINA ROSSINI AND NATALIE GREEN, PUBLIC KNOWLEDGE

EXECUTIVE SUMMARY

This will serve as an introduction to cybersecurity with a particular focus on the policy aspect of cyber security, including how cyber security is addressed in international relations and the impact cyber security has on human rights. By the end of the module, you should be able to answer the following questions:

- What role do "definitions" play in cybersecurity debates, discussions, and policy decisions?
- What are the main human rights concerns when dealing with cybersecurity?
- Are there international laws and standards that apply to cybersecurity? Do they address human rights concerns?
- How is cybersecurity addressed regionally and internationally?

BACKGROUND: HISTORY AND DEFINITIONS

Since the first computer worm was unleashed in the late 1980's to the recent 2014 Sony Pictures Entertainment hack, the security and stability of cyberspace, including the Internet, are often cornerstones from which discussions around cybersecurity, Internet governance, and Internet freedom begin. Threats to cybersecurity can include computer viruses, spam, identity theft, data breaches, denial of service attacks, and cybercrime. Attackers can range from hackers to activists to petty criminals to businesses to national governments. With over 370 million people falling victim to cybercrimes each year[1] and tens of thousands of known viruses in existence[2], the threats to our security are real - but so are the threats to our human rights online. Before looking at the human rights concerns in relation to cybersecurity, let's take a quick look at the outward expressions of cybersecurity.

In practice, outward expressions of cybersecurity include domestic public policy and laws (creation of cybersecurity agencies, such as the United States' Cyber Command), international public policy discussions (talks around creating an ITU/UN cybersecurity treaty), private business practices (anti-virus software, notification programs by ISPs, firewalls, etc), online surveillance (often by governments), and technical community practices aimed at maintaining the critical infrastructure of the Internet (Internet Engineering Task Force is one of these independent technical agencies).

1 http://www.pcmag.com/article2/0,2817,2425118,00.asp
2 https://www.uhd.edu/computing/helpdesk/documents/virusfacts.pdf

When talking about cybersecurity, what exactly do we mean? As you'll soon realise, there are a variety of definitions and terms that are used by cybersecurity firms, governments, international organisations, human rights activists, and others for different means, though they vary by a few words.

DEFINITIONS

In fact, a great example is the term cybersecurity itself, which the European Union defines as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure"[3]. The ITU defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets"[4]. Another example is the definition developed by the Freedom Online Coalition's cybersecurity Working Group "An Internet Free and Secure" based on the ISO 27000 standard, "Cybersecurity is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to preserve the security of persons both online and offline."[5]

The Internet Society (ISOC) has pointed that cybersecurity is "a catchword" that is "frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and "solutions" ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity."

As compared to many other areas of international relations or Internet-related topics, there is a void of concrete internationally-agreed upon definitions for phrases and definitions used to discuss cybersecurity. The definitions of 'information security', 'cybersecurity,' 'cyber-warfare', 'cyber-surveillance' and many others have not been agreed upon in a binding, standard setting international body or agreement. That means these terms are used by different actors in different ways, thus making policy discussions more confusing and making it easier for some governments to violate basic rights in the name of a broad 'cybersecurity' threat. In 2014, the Swiss government funded a project to consolidate cybersecurity related definitions in the Global Cyber Definitions Database. Before you continue, use the database to look up the various definitions of each of the following, as these words are crucial to your understanding of the basics of cybersecurity:

- Cybersecurity
- Internet security
- Information security
- Critical infrastructure
- Cyber space
- Cybercrime
- Cyber warfare
- Cyber threat
- Hacktivism

3 http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
4 http://www.itu.int/online/termite/index.html
5 https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/

BRIEF OVERVIEW WHERE CYBERSECURITY IS BEING DISCUSSED

HOW CYBERSECURITY IS ADDRESSED AT THE NATIONAL LEVEL

Cybersecurity involves helping protect the information that you, me, governments, businesses, and others keep online or in cyberspace, including communications (email, video messaging), finances (credit card information on websites like Amazon or the account numbers and information you use for e-banking), personal data (social security number, medical records on healthcare website), military secrets, and much more. Cyber incidents can also cause physical damage to critical infrastructure and networks as evidenced by the Stuxnet malware discovered in 2010 that targeted and destroyed some of centrifuges at the Natanz nuclear facility in Iran.

It is under this backdrop that cybersecurity threats and the risk of cyber attacks that could leak confidential military secrets or damage a country's economic/political infrastructure have garnered large attention not just as an Internet-related issues, but also as a national security issue. Other examples of national security threats throughout the world include nuclear weapons proliferation and war.

The United States, Russia, Japan, Kenya, European Union countries, are among the many countries that have declared the issue of cybersecurity, and specifically cyber attacks against their governments and citizens as a national security threat and developed national **cybersecurity strategies or initiatives.** Such cybersecurity initiatives and strategies normally outline the country's primary goals, concerns, set of principles or norms, and actions to be taken related to cybersecurity. Initiatives also can set up the creation of new agencies to deal with cybersecurity domestically or outline the role of already existing agencies, such as law enforcement, military, defense and foreign affairs ministries, in implementing cybersecurity policies. Cybersecurity initiatives, such as the United States' also support the development of **public-private partnerships (PPPs)** between government agencies and private sector companies, such as Internet Service Providers (ISPs), critical infrastructure owners, and technical companies around implementing cybersecurity measures across sectors. While governments mostly create and develop the cybersecurity initiatives, they may also consult technical experts, private businesses, and civil society for recommendations on how to improve strategies.

In discussing cybersecurity, you will most often hear about cybersecurity laws and measures to defeat **cybercrime**. In general, cybercrime refers to crimes that take place with or deal with computers and cyberspace, but also to traditional acts of crime (such as drug trafficking) that take place online. Within many countries' national cybersecurity initiatives and strategies are specific references and initiatives towards combating cybercrime based off current law enforcement and criminal justice systems. As you'll see in the **Human Rights Concerns About Cybersecurity** section, governments and surveillance agencies alike often cite "combating cybercrime" as a reason to support overarching cybersecurity and cybercrime laws and practices.

CYBERSECURITY AT THE INTERNATIONAL LEVEL

While domestic laws and practices have been working to address cybersecurity concerns, the issue of cybersecurity is a truly transnational issue. Cyberspace is

a borderless series of networks, and cybersecurity threats move across military, political, and geographical boundaries. Attackers can be highly targeted or they can choose to unleash a threat that could impact dozens of countries and millions, or billions of people at once. As domestic initiatives, and countries without extensive cybersecurity plans, have failed to stop the growing number of highly sophisticated transnational viruses and threats, international cooperation around cybersecurity issues is becoming the focal point of civil society, governments, private sector, and others.

While some have pointed to international cooperation as the key to a secure Internet in the future, many countries have yet to set their own domestic policies that properly address cybersecurity, and other countries have adopted overarching policies that directly violate human rights. In fact, an often ignored factor in cybersecurity debates on the international scene is the role that states themselves play in exacerbating cybersecurity threats and concerns. The United States, European Union countries, Iran[6] , Israel [7], China, and Russia[8] have all been accused of launching cyber attacks against other states and of creating a 21st century arms race - the **cyber arms race.**

At the international organisation level, the issue of cybersecurity first came to the UN's agenda when the Russian Federation introduced a draft resolution in the First Committee of the UN General Assembly that was later adopted in 1998. Since 2010, three Groups of Governmental Experts (GCEs) have been tasked by the UN General Assembly to research and report on existing and potential threats to cybersecurity and recommendations on how to address them. In their 2010, 2011 and 2012/2013 reports, GCEs concluded, amongst a number of things, an increased need for "international cooperation against threats in the sphere of ICT security" with input from civil society and the private sector, but also emphasised that "State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments." In 2014, the UN adopted a new resolution on cybersecurity, and it is expected that another GCE report, possibly influenced by revelations of United States and United Kingdom mass online surveillance, will be issued in 2015.

Another important move that was made at the UN was the letter sent by Russia, China, Uzbekistan, and Tajikistan to the UN Secretary-General calling for an International Code of Conduct for Information Security. Though the letter recognizes the role of human rights in cybersecurity, it also emphasises the need for states to curb "the dissemination of information that incites terrorism, secessionism, extremism, or undermines other countries' political, economic and social stability," a clause that is worrying to free expression advocates. The UN Institute for Disarmament Research, the UN Office on Drugs and Crime, the International Telecommunications Union, and the UN Human Rights Council have all made various statements and pushed for initiatives related to cybersecurity.

At the regional and bilateral level, almost every single world region has held policy discussions, and some have even issued treaties, on cybersecurity. Both the North Atlantic Treaty Organisation (NATO) and the Organisation for Security and Cooperation in Europe (OSCE) have adopted principles or tasked member states to build collaboration around cybersecurity issues such as, capacity building, cybercrime, and the applicability of international law (including human rights law) to cybersecurity. In 2013, the European Union (EU) adopted the Cyber Strategy of the European Union: An Open, Safe and Secure Cyberspace which emphasised

6 http://www.businessinsider.com/iran-is-officially-a-real-player-in-the-cyber-war-2014-12

7 http://f.cl.ly/items/0t073Y3i3P0v2o2x0q39/Baseline%20Review%202014%20ICT%20Processes%20colprint.pdf

8 http://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html

protecting freedom of expression and privacy in core cybersecurity principles, but also tasked a number of other bodies in Europe including the European Parliament, the European Network and Information Security Agency, and others to provide further assistance, information sharing, and training to EU member states.

To read more about these regional efforts including those in Asia, Africa, and Latin America and global bilateral efforts in cybersecurity, consider reading pg. 15-25 in "Baseline Review of ICT-Related Processes and Events."

Other than the conventions and decisions already mentioned, the issue of cybersecurity has become increasingly central within the spectrum of traditional multistakeholder and multilateral internet governance spaces. In summer 2013, the Internet governance community was shaken by Edward Snowden's revelations on US and UK mass surveillance, and the push for increased cooperation and shaming related to cybersecurity increased dramatically. As already mentioned, within months of the revelations, Brazil and Germany sponsored a resolution at the UN on "The Right to Privacy in the Digital Age," which was eventually adopted in 2014. In April 2014, Brazil hosted Netmundial, the Global Multistakeholder Meeting on the Future of Internet Governance. The non-binding outcome document that was created with civil society input called for international cybersecurity policy decisions to be held in multistakeholder fora with engagement from all interested parties, including civil society. While non-binding, the Netmundial outcome document has been a tool for governments and civil society who have pushed against international multilateral cybersecurity treaties and decision-making.

The International Telecommunication Union (ITU) is the multilateral UN agency tasked with issues related to information and communications technologies (ICTs). Every four years, the ITU hosts a plenipotentiary conference in which the 193 member states decide on the future of the organisation. This meeting is open only to member states and the delegation members that these states choose. After the UN-sponsored World Summit on the Information Society (WSIS) global events were held in 2003 in Geneva and 2005 in Tunis to allow people and stakeholders around the world to give their input on issues related to Internet access, security, and privacy, the ITU was granted a role in facilitating WSIS Action Line item c5 "Building Confidence and Security in the Use of ICTs". Governments such as Russia and China have been able to use this Action Item role to push for increased consolidation of cybersecurity issues within the ITU.

In 2007, the ITU adopted a Global Cybersecurity Agenda as a framework for international engagement between Member States on cybersecurity issues. Four of the ITU's resolutions (resolutions 130, 174, 179, and 181) relate to cybersecurity, and leading up to the 2014 ITU plenipotentiary conference held in Busan, South Korea, a number of country delegations, including Russia and Arab states, suggested modifications to the resolutions to increase the ITU's role in cybersecurity.

At the annual multistakeholder UN-sponsored Internet Governance Forum (IGF), an increasing number of workshops and discussions have focused on cybersecurity, but the non-binding, non-outcome based fora have not yet produced any positions or policy statements on cybersecurity-related issues. In addition to the IGF, the multi-stakeholder conference series first held in London in 2011, called the "London Conference on Cyberspace" was launched with support from the UK government. The conference is an opportunity for all interested stakeholders to engage in discussions and debates on cybersecurity issues, and has since been held in Hungary and South Korea. The 2015 conference was held in the Netherlands.

AN INTERNATIONAL TREATY ON CYBERSECURITY?

Leading up to the ITU's 2014's plenipotentiary conference, there was also discussion of a cybersecurity treaty being negotiated, but that never came to fruition. Even so, discussions of an international convention or treaty on cybersecurity with a focus on expanding the already existing 2001 Council of Europe Convention on Cybercrime (aka the Budapest Convention) have been raised throughout the world, especially post-ITU plenipotentiary[9] . The Budapest Convention, though focusing specifically on cybercrime and not all cybersecurity issues, has been ratified by 44 countries (mostly European, but also including Australia, the Dominican Republic, Japan, Mauritius, Panama, and the United States). The Budapest Convention's primary goal is to harmonise domestic criminal law to certain areas of cybercrime in order to create an international norm for enhanced cooperation on cyber crime. In the convention, illegal access and interception, data and system interference, misuse of devices, computer-related forgery and fraud, child pornography, and some instances related to copyright are considered cybercrime offenses.

Arguments in favour of creating a cybersecurity treaty, with remnants of the Budapest Convention, include that the creation of an Internet-specific treaty could lead to creating laws of cyberwar, similar to conventional war treaties that may restrict attacks against citizens or children. Others have claimed that the creation of a cybersecurity treaty would likely be closed to the public and civil society and become highly politicised in an international organisation, such as the U.N. There's also significant worry that an international treaty related to issues of security would not fully take into consideration human rights law or would make exceptions to human rights law. Unsurprisingly, the issue of *definitions* is especially relevant as many countries use terms such as *cybersecurity* and *information security* interchangeably or may define *attackers*, *hacktivists*, and other key words differently. The harmonisation of such terms could lead to the acceptance of broad cybersecurity terms that could be used to further violate basic human rights in the name of security.

That's why a variety of civil society groups, including the digital rights coalition Best Bits, actively petitioned against increasing the ITU's role in cybersecurity and the development of an international cybersecurity treaty. The ITU's role in cybersecurity is often rebuked by governments and civil society for a number of reasons including lack of technical-expertise at the ITU, the broad language of proposed cybersecurity treaty language, the number of other UN agencies and other fora (both multistakeholder and multilateral) that could address cybersecurity, and the lack of transparency and participation opportunities, especially for civil society. Others look at the debate of the ITU's role in cybersecurity as a part of ongoing cyber-related issues and attacks between countries, including the United States and Russia.

HUMAN RIGHTS CONCERNS ABOUT CYBERSECURITY

Though some domestic and international laws attempt to address human rights considerations in forming cybersecurity standards, the negative impact on human rights caused by overarching and broad cybersecurity laws and principles has become apparent to civil society advocates and others.

When talking about human rights, we are mostly referring to those rights

9 http://f.cl.ly/items/0t073Y3i3P0v2o2x0q39/Baseline%20Review%202014%20ICT%20Processes%20colprint.pdf

guaranteed under the United Nations' Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), including **freedom of expression, freedom of speech, the right to privacy, freedom of opinion,** and **freedom of association** as some of the most basic rights of all humans. In response to the creation of the Internet as a new platform for expressing basic human rights, the UN Special Rapporteur on Freedom of Opinion and Expression and free expression rapporteurs from Europe, Latin America, and Africa signed a joint declaration confirming that **"freedom of expression applies to the Internet"** in 2011. In July 2012 the UN Human Rights Council further confirmed that **"the same rights that people have offline must also be protected online,"** thus making the formerly mentioned human rights declarations of UDHR, ICCPR applicable to the Internet.

A number of cybersecurity laws and measures that have been taken by individual countries could have a negative impact on **online speech** and **freedom of expression** by directly infringing upon such rights or creating a chilling effect on the desire of people to express their rights. The Anti-Cyber Crime Law of Saudi Arabia and its vague clause on "protection of public interest, morals, and common values", have been used to crack down on online speech and freedom of expression by imprisoning bloggers and others for voicing different opinions, insulting public officials, or supporting forces other than the government in power. In 2012, the Philippines approved the Cyber Crime Prevention Act that addressed legitimate cybersecurity concerns, such as child pornography and spam, but also criminalised libel. Though the provision on libel was eventually dropped the following year, its original intentions were enough to worry Filipino activists and lawmakers into drafting a bill called Magna Carta for Philippine Internet Freedom in direct opposition to the law. In addition to cybersecurity laws developed by governments, firewalls developed by IT businesses and companies (with government support) can be used to block specific websites and content, leading to **online censorship.**

Just a week after the Charlie Hebdo attacks in Paris in early 2015, Prime Minister David Cameron announced his support to ban encrypted message services, such as Whatsapp, if British intelligence agencies were not given increased access to messages and user data. Cameron stressed the need for increased access to encrypted messages as a means to protect the UK from terrorist attacks. Banning encrypted message services could be seen as a violation of both the right to privacy and online anonymity in the name of national security, through cybersecurity and online surveillance. The **right to privacy** allows for all people to keep information about themselves out of the hands of those they don't want to have the information. **Online anonymity** is the right to say something online without having it be connected to your real identity, and both are important for maintaining the Internet as a platform for free expression[10] , especially for political or social dissenters or those who want to avoid harassment, imprisonment or worse. In 2013, the UN Special Rapporteur on Freedom of Opinion and Expression issued a report on the impact of surveillance on human rights, noting that "the use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is a serious concern."

In 2009, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism issued a report that stated that Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which states that "no one shall be subjected to arbitrary or unlawful interference with his privacy" is actually "flexible enough to enable necessary, legitimate, and proportionate restrictions to the right to privacy," but only in cases where a law is already in place that outlines when privacy can be violated, when it protects the rights of others, and/or when is in line with necessary and proportionate principles. **Necessary and proportionate principles**, and similar terms are often used to distinguish how surveillance practices, including online

10 https://www.eff.org/issues/anonymity

surveillance, can be done within international laws and human rights-based principles, including with proper public oversight, due process, and a system for user notification.

In addition to freedom of expression, speech, privacy, and anonymity comes the issues of ethnically and religiously discriminatory practices and standards within cybersecurity laws in the West against Muslims and the validity of online protest, such as hacking, as a cybersecurity threat.

Though cybersecurity threats are real, the ability to communicate anonymously, voice disapproval, protest, and have discourse without fear of persecution is an important part of human rights that all people are guaranteed. While state based agencies and actors have control and access to the Internet and its data, some have claimed that checks and balances are needed, such as oversight committees, international laws, and internationally agreed upon definitions for key words.

ROLES OF STAKEHOLDERS IN CYBERSECURITY

In talking about the multilateral and multistakeholder ways in which cybersecurity is addressed, it is important to understand what role different stakeholders play in these discussions. Ideally, governments, the private sector, civil society, and the technical community would all play equal roles in creating and implementing cybersecurity policies and decisions, but realistically this isn't always the case.

Traditionally, governments play the primary role in creating the public policies and laws that regulate and determine cybersecurity measures domestically, sometimes with non-governmental input, but usually from private cybersecurity firms or industry. In addition, governments are also capable of launching and supporting cyberattacks of their own against other countries, and they are the only stakeholder guaranteed a say in the ITU and other international multilateral bodies. On the international stage, a handful of governments (previously mentioned) have pushed for increasing the role of governments and intergovernmental organisations in cybersecurity.

Private sector companies, including ISPs and the IT sector are crucial because of their role in creating and maintaining the technologies (computers, tablets, etc) on which cybersecurity issues arise. Governments often consult these companies when making public policy decisions in order to ensure that cybersecurity standards can be applied to various technologies. At the same time, the number of cybersecurity firms in the private sector is quickly growing, and they often profit from strict cybersecurity policies. Similar to private sector companies, the technical community has the technical expertise and understanding of the Internet and is often cited by governments when developing cybersecurity policies. The technical community, including the Internet Engineering Taskforce also works independent of governments and politically-motivated cybersecurity measures to help ensure the security of the Internet's critical infrastructure .[11]

Similar to other areas of Internet governance, civil society's role in cybersecurity has just begun to take off in recent years. On the one hand, civil society groups have pushed for further inclusion at international discussions and domestic policy-making meetings, but others are calling for civil society to create their own positive agenda for cybersecurity policy and norm making. Civil society has a unique role in being able to advocate for cybersecurity policies from a human rights-based approach. In 2011, CitizenLab developed a report outlining the possible role

11 See pg. 106: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

for civil society in cybersecurity, and in 2013, the Association for Progressive Communications created a similar agenda. Both reports emphasise the importance of civil society in bringing to light human rights considerations in all cybersecurity-related discussions, but also address the need for civil society to call for evidence-based cybersecurity decisions and practices.