Why It Is Time to Start Treating Cybersecurity Like a Human Rights Issue

Prof V K Rai[1], Santosh Kumar Sonkar[2]

[1]Political Science Department, University of Allahabad, Prayagraj
[2]Research Scholar (SRF), Political Science Department, University of Allahabad, Prayagraj

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: Cybersecurity is much more than an IT topic"

Stephane Nappo

Abstract

The most important invention of the god is the man which has been enriched with various attributes and this man has successfully utilized such features for the betterment of himself as well as the society. But as said by a prominent jurist Voltaire "*that with great power comes great responsibility*" and also that everything has merit as well as demerit which is responsible for maintaining the equilibrium of the society. Likewise with the invention of cyber world the problem of compromising and hence the issue of cyber security is stem out and along with the it a major and serious concern of the developing nations is that of hindrance to Human Rights due to such intrusion of the cyber world by human beings. This above article talks about the concern that why it is need of the society to not only treat cybersecurity as cyber issue but also as a Human Rights issue for which answers to the question that how can be cybersecurity be taken into the ambit of Human Rights.

Introduction

"Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience"

Stephane Nappo

Rising cyber security threats were cited as a major threat to international security by Secretary-General António Guterres in his opening remarks at the high-level opening of the UN General Assembly in 2017. Cyber attacks have shut down hospitals, disrupted electrical grids, paralyzed major cities, and even jeopardized the integrity of democratic processes in addition to the threat of cyber war. The average global cost of a data breach to a company in 2019 is estimated by a recent report commissioned by IBM to be USD 3.92 million.

It is understandable why governments, businesses, and the technical community are putting more emphasis on enhancing cyber security as threats to it grow more frequent, sophisticated, and serious. However, efforts to advance cyber security frequently neglect or, worse, see human rights as a barrier to cyber security. This is a risky and incorrect assumption. We need to start treating the issue of cyber security as one of human rights.

Definition of cybersecurity

”If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”

Bruce Schneier

Although there isn't a single definition of cyber security, the one created by the Freedom Online Coalition's (FOC) "Internet Free and Secure" working group, which was made up of technologists, human rights specialists, and government officials, is instructive. The FOC working group defines cyber security as "the preservation of the availability, confidentiality, and integrity of information and its underlying infrastructure through policy, technology, and education in order to enhance the security of persons both online and offline".

Why human rights are a concern in cybersecurity

“Digital Rights are Human Rights . As our lives become more digital , denying people access to the interest , or the tools to navigate it safely, is becoming a violation of basic Human Rights ”

Nighat Dad

It is simple to see how threats to cyber security, or cyber insecurity, can constitute human rights violations using the FOC definition of cybers ecurity as a foundation. Network shutdowns, for instance, which deny access to information and its supporting infrastructure, infringe on a number of rights by unreasonably limiting people's freedoms of expression, association, and peaceful assembly as well as their enjoyment of a number of economic, social, and cultural rights. In 2018, 196 internet shutdowns in 68 countries were recorded.

There are countless instances of information confidentiality being violated, including the right to privacy and other rights, through data breaches carried out for monetary gain, widespread government surveillance, or targeted attacks against journalists or human rights advocates. Violations of serious human rights, such as detention, torture, and extrajudicial killings, are associated with breaches of the confidentiality of communications through surveillance. The surveillance of Saudi dissident Omar Abdulaziz, which contributed to the extrajudicial killing of Saudi journalist Jamal Khashoggi, is one instance of a particularly egregious case. A lawsuit claims that in the months prior to Khashoggi's murder, the Saudi Arabian government installed spyware on Abdulaziz's cell phone, jeopardising the confidentiality of his communications with Khashoggi about opposition projects.

Although the majority of people—even those for whom meaningful internet access is difficult—are likely to experience some form of cyber insecurity throughout their lifetime, not everyone experiences it in the same way. Human rights advocates, journalists, and individuals in marginalised or vulnerable positions—for example, due to their religion, ethnicity, sexual orientation, or gender identity—can face particular risks. For instance, because of their position in society, they are more likely to be the target of governmental or lateral surveillance, and the repercussions of larger threats like data breaches or network shutdowns are frequently more severe for them.

The risks associated with cyber security will only grow as more people and devices are connected. Unfortunately, governments either fail to prioritize human rights in cybersecurity discussions or, worse yet, use cyber security as a justification for expanding internet censorship.

The Securitisation of cyber technology

" It's simply unrealistic to depend on secrecy for security in computer software. You may be able to keep the exact workings of the program out of general circulation, but can you prevent the code from being reverse-engineered by serious opponents? Probably not. The secret to strong security: less reliance on secrets."

Whitfield Diffie

The development of cyber security laws, policies, and norms frequently occurs in highly secretive, securitized contexts without the assistance of civil society or human rights expertise. This is in opposition to the multistakeholder model of internet governance, which depends on the active participation of governments, businesses, non-profits, and international organizations. Importantly, this strategy disregards the knowledge and oversight necessary to uphold human rights. Frequently, cyber security discussions take place within the walls of intelligence services or other governmental or military organizations that are shielded from public view or oversight. Sometimes, cyber security is also equated with national security, which is viewed as a sacred space in which governments can act however they please without interference from the public or even oversight. As a result, human rights frameworks are frequently absent from cyber security law, practises, and policies, making them vulnerable to power abuse.

International cyber security debates miss the mark

It is well established that digital technologies are subject to international human rights law. However, international human rights law is rarely, if ever, a topic of discussion when it comes to cyber security. This is in part because international conversations on cyber security typically address the problem of state-on-state attacks and fall under the umbrella of international security and disarmament. However, the tone of these conversations and the resulting norms have an impact on how states approach cyber security at the federal level. The Shanghai Cooperation Organization (SCO), which has been working to advance the idea of extending national sovereignty and information control in cyberspace, is particularly concerning in this regard.

Since 2013, the UN has maintained that cyberspace is subject to international law, including international humanitarian law and international human rights law. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security further elaborated that respect for human rights and fundamental freedoms is seen as being "of central importance" in 2015 and advised states to adhere to the UN resolutions that are related to the right to privacy in the digital age and human rights on the internet. International humanitarian law has received the majority of attention while the international community has become stuck on how international law operates in cyberspace. This strategy is flawed for a number of reasons. First, international human rights law is always in effect, whereas international humanitarian law only applies during times of armed conflict (in peace and war). International human rights law is more frequently the applicable framework given that the majority of the different types of cyber insecurity are experienced in times of peace (or at least when there isn't a declared cyber war). The idea that states are engaged in an ongoing cyber conflict may be advanced by focusing discussions on international humanitarian law, which could result in an increase in cyber attacks. Third, international humanitarian law is a body of law that allows more harm to the public than is typically permitted.

The development of norms for responsible state behaviour in cyberspace should take into account the specific guidance provided by international human rights mechanisms. For instance, UN Special Procedures reports explain why strong encryption is required for the confidentiality of information and how network shutdowns violate human rights law and unreasonably obstruct information availability. The UN Guiding Principles on Business and Human Rights, which define the obligation of the private sector to respect human rights, mitigate negative effects, and make good on harm, are a well-established set of standards under international human rights law. This is a crucial point, given that the majority of the hardware, software, and infrastructure that make up the internet are owned and/or operated by the private sector.

Cyber Security for whom

The most pernicious threat is that states will use the seriousness of cyber security threats as an excuse to violate human rights directly through the use of their power in cyberspace. It is crucial to consider security for whom when evaluating a cyber security framework. protection from what? and how is security achieved? Answers to these questions all too frequently show that the state views security as its own defense against political instability, employs disproportionate force to ensure its own survival, and then becomes the source of insecurity.

A cyber security law was passed in Vietnam last year that enables the government to compel technology companies to hand over potentially enormous amounts of data, including personal information, and to censor users' posts, to name just a few examples. A cyber security law that requires businesses to censor "prohibited" information, restricts online anonymity, including by requiring real name registration, and requires the storage of Chinese users' data within the nation was adopted in China the previous year. In Israel, a bill known as the Cyber Security and National Cyber Directorate Bill would grant the government broad new authority to break into and steal data from any person or organization deemed to pose a threat to cyber security. Early this year, the Venezuelan government proposed the Constitutional Law of Cyberspace, which asserts Venezuelan sovereignty over cyberspace and, among other measures to increase state control of the internet, would require messaging service providers to censor content without a prior judicial order or respect for the minimum due process guarantees.

Each of these instances shows how a government is using security as an instrument at the expense of human rights, particularly the rights to privacy, freedom of expression, association, and assembly. Incidentally, these examples also show how cyber security, or the accessibility, confidentiality, and integrity of data and the underlying infrastructure, are being sacrificed in the name of security.

Putting cybersecurity on right tracks

It's time to start thinking of cyber security as a human rights issue in order to protect human rights in this digital age.

First, it's important to refute the widely held belief that human rights pose a security threat. The claim that encryption, which is essential for exercising the right to privacy, makes it harder for law enforcement to carry out its duties is arguably the most frequently used example of how human rights conflict with security. Governments frequently argue in favour of introducing backdoors and reducing encryption in order to give law enforcement access to encrypted communications. However, experts concur that it is impossible to give one government access to encrypted communications without also giving it to all other governments and bad non-state actors. Or to put it another way, compromising cyber security for law enforcement means compromising security for everyone, endangering everyone's human rights. This is due to the fact that human security, which is a fundamental human right, is inextricably linked to cyber security. Human rights and cyber security are interdependent, complementary, and reinforce one another. To effectively promote freedom and security, both must be pursued.

Second, it is crucial to integrate human rights perspectives into cyber security laws, policies, and procedures. Never should the threat of cyber insecurity be used as an excuse to violate human rights. Instead, the protection of human rights should be at the forefront of cyber security policy development because it is understood that individual and collective security is at the core of cyber security. It is crucial to ground cyber security discussions in international human rights law at the global level. In order to ensure that cyber security policies and practices are founded upon and fully consistent with human rights—in other words, that cyber security policies and practices are rights-respecting by design—the Freedom Online Coalition "Internet Free and Secure" working group developed a set of cyber security- and human rights-focused policy recommendations. These recommendations, which have received support from 30 FOC governments and more than two dozen NGOs, are a helpful place to start when incorporating human rights considerations into cyber security practices and policies.

Third, commercial companies need to uphold the human rights, and governments also need to hold them accountable. The UN Guiding Principles on Business and Human Rights provide the necessary framework, but there is a need for closer examination and regulation of technology firms, both those that supply the tools and programmes used to launch cyber attacks and those that act as the first line of defense against them. They should also conduct cyber security due diligence to review the governance, processes, and controls that are used to secure the information they process, in addition to conducting human rights impact assessments to identify, understand, assess, and address the negative effects of their policies and practices on the enjoyment of human rights. Businesses have advanced self-regulatory initiatives like Microsoft's Cyber security Tech Accord, which addresses cyber security threats that jeopardize people's rights but lacks an explicit human rights framework and has some gaps.

In order to prevent and lessen human rights violations brought on by cyber security, governments can take additional steps to regulate the technology sector. A recent call for a moratorium on surveillance technology came from the UN Special Reporter on the promotion and protection of the right to freedom of opinion and expression. Such courageous actions are required to ensure that businesses are not making money off of violations of human rights or carelessly handling people's data, not just for the surveillance technology sector but for the technology sector as a whole.

Fourth, human rights and technical expertise must be incorporated into multidisciplinary, inclusive, and multistakeholder cyber security processes. This entails expanding the scope of cyber security beyond the purview of national security and intelligence organisations and dispelling the notion that cyber security is primarily a national security issue. Given how frequently citizens are asked to make sacrifices in the name of national security, it is essential that the justifications for those sacrifices be examined for their necessity and proportionality; that independent oversight be provided of responses to threats to national security to ensure that these responses are justified; and that there be increased transparency and public discourse to prevent national security from being confused with regime security.

Therefore we can conclude that Human rights and security are faced with new, unforeseen challenges thanks to digital technologies, which will necessitate more documentation, research, and analysis.

Human rights and cyber security will both suffer until they are recognized as complementary and mutually reinforcing.

"It is not data that is being exploited, it's people that are being exploited".

Edward Snowden

"Security used to be an inconvenience sometimes, but now it's a necessity all the time"

Martina Navratilova

References

1. Cherian Samuel, ―Cybersecurity and Cyberwarfare 650 *Seminar* 26 (2013).
2. Eric A. Fischer , *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, CRS Report RL32777
3. Hannibal Travis, Cyberspace Law: Censorship And regulation of the internet, 1 (Taylor &Francis Group, 2013, New York)
4. Mr. Karra Kameswara Rao " *Human Rights And Cyberspace Use And Misuse* " Bharti Law Review , July –Sept, 2016
5. Nina Godbole, Sunit Belapure, *Cyber Security: Understanding Cyber Crimes,Computer Forensics and Legal Perspecives*, 283 (Wiley India Pvt.Ltd.New Delhi, 2011).
6. Prashant Mali, ―Cyber *Law & Cyber Crimes*‖ (Snow white Publication, Mumbai, second edn., 2015).
7. T.M Samuel, Maria Samuel, Computer Crime and Information Technology Misuse,152(commonwealth Publication, New Delhi, 2008)
8. Vittorio Fanchiotti , Jean Paul Pierini " *Impact of Cyberspace on Human Rights and Democracy*" 2012 4th International Conference on Cyber Conflict
9. Whitman and Mattord, *Principles of Information Security* (Thomson course technology, Canada, 3rd edn.,2009).
10. https://psu.pb.unizin.org/ist110/chapter/12-2-computer-security/ visited on March 20, 2023
11. https://www.legalserviceindia.com/legal/article-4724-cyber-security-and-cyber-crime-infringes-human-rights-.html visited on March 21, 2023
12. https://curiousforlaw.com/cyber-security-and-privacy-a-responsibility/ visited on Febuaray 24, 2023
13. https://www.thelawgurukul.com/post/cybercrimes-and-the-regulation-of-cyber-laws visited on March 24, 2023
14. https://www.quora.com/What-are-the-basic-concepts-of-cyber-security visited on March 24, 2023