PHRG
PEACE HUMAN
RIGHTS GOVERNANCE

Volume 4, Issue 3, November 2020

Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups

Pavlina Pavlova

Policy Papers

DOI:

10.14658/pupj-phrg-2020-3-4

How to cite:

Pavlova, P. (2020) 'Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups', *Peace Human Rights Governance*, 4(3), 391-418.

Article first published online

November 2020

*All research articles published in PHRG undergo a rigorous double-blind review process by at least two independent, anonymous expert reviewers

PADOVA UP

PHRG 4(3), November 2020

Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups

*Pavlina Pavlova**

Abstract: This article analyses the human rights dimension of security as a prerequisite for designing a comprehensive cybersecurity framework. As a result of "securitisation" of this field, there has been a prevailing image of the need to sacrifice freedoms for the objective of national security – with the right to privacy being among the most contested rights in cyberspace. compromised accounts, phishing, internet blocking, filtering, censorship practices, information gathering, excessive electronic surveillance with facial software, data collection and profiling – these are some of the practices with potential for infringing on this right. But risks in cyberspace are not experienced evenly by everyone. Human rights defenders, journalist, activist, minority and marginalised groups are particularly at risk. They have been intentionally on a larger scale and with far-reaching consequences not only for their digital but often physical and psychosocial security. The conclusion will reason that there is a need for more safeguards as countervailing measures against possible human rights violations. Efficient translation of human rights standards into cyberspace realm needs to be ensured together with greater regulation and accountability. Beyond creating adequate legal and regulatory protection, building necessary awareness and skills for digital security is a measure of key importance.

Keywords: *Human Rights, Cybersecurity, Human Rights Defenders, Security Risks, Internet Governance*

* Consultant at the OSCE Office for Democratic Institutions and Human Rights (ODIHR), email: Pavlina.Pavlova@odihr.pl

Introduction

Cyberspace has long been understood as an unlimited space, where established laws are not applicable, and states have only limited powers. It was hoped that cyberspace could provide for greater connectivity and the creation of a public space that would help to overcome some of the restrictions of the 'offline world': geographical distance, legal restrictions and government control. But with its growing omnipresence, technological sophistication, the dominance of powerful private actors, and mounting political stakes, cyberspace is increasingly considered to be one of the main geopolitical arenas (Barrinha and Renard 2020). This article focuses on what this shift represents for targeted groups, with a strong emphasis on case studies of Human Rights Defenders (HRDs). The United Nations General Assembly has adopted the Declaration on Human Rights Defenders in 1998, recognising the right of individuals and organisations to voluntarily or professionally strive to preserve, promote or propose human rights as they relate to themselves, their communities or their causes (UN General Assembly 1999). The term refers to anyone promoting or defending any of a vast array of rights, which may include civil and political rights such as freedom of speech, justice for survivors of abuse, transparency and anti-corruption, or greater political participation. The recognition of the importance of their work under international law, as well as under the laws of numerous states, gives HRDs an additional layer of protection to carry out their work (Higson-Smith et al. 2016, 10). However, it needs to be taken into consideration that similar vulnerabilities are also being experienced by other targeted individuals and groups-at-risk, notably journalists and activists as well as marginalised, discriminated and non-conformist groups.

The possible abuses of technological tools range from compromised accounts, phishing, internet blocking, filtering, censorship practices, information gathering, excessive electronic surveillance, data collection and profiling, or biometrics identification without non-compliance with due process guarantees. These are some of the common practices that violate human rights or limit their full enjoyment (Higson-Smith et al. 2016, 73-74). Some of the most contested issues in cyberspace are the right to privacy, freedom of thought, conscience and religion or belief, freedom of opinion, freedom of expression and information, freedom of peaceful assembly and association, and the right to equality before the law (Hildebrandt 2013,19). This article focuses on the threats to HRDs' security that stem from deliberate efforts of some governments to limit their activities and those introducing restrictive cybersecurity measures and new technologies which

can potentially infringe on human rights and accordingly interfere with HRDs' ability to carry out their work.

The case studies of HRDs analysed below have been selected because they represent a vulnerable group in cyberspace and to create a substantial empirical basis for illustrating what cybersecurity means for individuals and communities-at-risk. By doing so, the paper demonstrates that security cannot be guaranteed without safeguards for fundamental rights and freedoms. While the attention is placed on the cases involving states' interference, it should be taken into consideration that HRDs face additional risks from private actors, both in form of direct attacks or by developing and deploying technological tools and platforms that can be misused against them. However, states remain the most powerful actors in cyberspace. Importantly, they have obligations and duties under international law to respect, to protect and to guarantee human rights. The first obligation means that States must refrain from interfering with or curtailing the enjoyment of human rights. The second requires States to protect individuals and groups against human rights abuses, and the obligation to fulfil means that States must take positive action to guarantee the enjoyment of basic human rights (UN no date).

The aim of this article is to highlight the importance of the human rights dimension of security and its complementarity with cybersecurity policies. While human rights violations in cyberspace have been highlighted in the relevant literature for more than a decade, and as will be outlined in the article, the idea of a human-centric approach on cybersecurity has also been recorded to some extent, this article contributes to the existing discussion by focusing on the examples of targeted groups to link their cases to a wider theoretical concept. Guided by approaches developed in the field of international relations, the paper challenges the dominant view that cybersecurity is exclusively a matter of national security. The main argument of this paper is that as a result of 'securitisation' of this field, the human rights dimension has been depreciated – with the right to privacy being among the most contested rights in cyberspace.

As outlined through examples of the interception of communications and compromised confidentiality of information, the denial of information and its underlying infrastructure, and the development and deployment of new technologies with a potential of infringing on human rights, one can argue that the current cybersecurity framework is not sufficient for guaranteeing people's security and safeguarding their rights. The conclusion will contend that taking into account the human rights dimension of security is a prerequisite for designing a comprehensive cybersecurity framework. To this end, there is a need for more safeguards as countervailing measures

against possible human rights violations. A swift and efficient translation of human rights standards into the cyberspace realm must be ensured together with stronger regulation and accountability. Beyond the creation of adequate legal and regulatory protection, building necessary awareness and essential skills for digital security is a measure of key importance.

In terms of methodology, this paper uses qualitative analysis of several case studies. The case studies have been selected because they illustrate the common issues and overarching, large-scale threat that HRDs face in cyberspace. The paper employs these cases with attention to the digital, psychosocial and physical security of the targeted groups or individuals. This case-based research design is particularly effective in exploring the intricacies of how the shortcomings in the cybersecurity framework affect human rights in cyberspace. Since case studies come with a risk of empirical myopia – since a small number of cases can be taken as indicative of all cases – more research is needed to further test the hypothesis outlined in this article.

To the goal of establishing the importance of the human rights dimension in the cybersecurity framework and the examples of human rights violations based on the cases of the groups-at-risk in cyberspace, the following structure will be used:

Section 1 offers the theoretical framework for cyberspace and cybersecurity. Section 2 looks closer into the human dimension of security, compares it to the prevailing national security approach and so explains its position within the current cybersecurity framework. In this context, Section 3 outlines which human rights are most affected in cyberspace and what steps have been taken to address this issue on the international level. Section 4 outlines what digital threats mean for the security of vulnerable groups in cyberspace on the example of HRDs as a prominently targeted group, clustering them into three main groups. Based on the analysis, the conclusion outlined in Section 5 proposes general recommendations to the existing cybersecurity normative, legislative and regulatory framework from the perspective of the human-rights centric approach.

1. Cyberspace and Cybersecurity: Theoretical Framework

The term 'Cyberspace' has evolved from the work of Norbert Wiener using word 'cybernetics' in 1948 the meaning of *'control and communication in the animal and the machine'*. The idea that people can interface with machines and that the resulting system can provide an alternative environment for interaction provided a foundation for the concept. It was further developed

in the work of William Gibson who officially coined 'cyberspace' in his 1982 collection Burning Chromeand (BBC 2016). A single common definition for cyberspace has never been established and many existing are vague or missing key components, risking that the derived terms will be meaningless or flawed. A definition acknowledging the importance of human users has been proposed by Ottis and Lorents (2011, 1) who describe cyberspace as *'a time-dependent set of interconnected information systems and the human users that interact with these systems'*. This framework understands cyberspace as an artificial space, created by humans for human purposes, and in this way recognises its inherently human dimension.

The prefix 'cyber' gained popularity and in academic literature and public discourse alike. Cybersecurity, cyber diplomacy, cyber politics, cyberlaw, cyberconflict, cyber ethics, cyber power, cyber deterrence, cyber-surveillance are just some of the examples of how the term 'cyber' has been used to describe almost anything that has to do with networks and computers'. The first listed term particularly resonated with the military terminology when cybersecurity took on the meaning of securing cyberspace and related vital infrastructure of states from external threats (Rout 2015). The national security accent on potential threats has led to the narrow understanding of cybersecurity that is heavily focused on restrictive measures as the way to greater security. Consequently, the human rights dimension faces downward pressure – making the contested human rights in the cyberspace – such as the right to privacy, the right to freedom of expression and information, the right to association and assembly – into a secondary concern (Taddeo 2013, 353). This continuous 'securitisation' of this field prevents a meaningful inclusion of a human-rights-centric approach (APC 2019). Therefore, it is necessary to broaden the understanding of cybersecurity beyond only a matter of national security to allow for the creation of a comprehensive cybersecurity framework.

As some definitions of cybersecurity can suppress, diminish or even oppose the human dimension, understanding how to approach the term is the first step to effective involvement. The definition introduced by the Internet Free and Secure Initiative (IFSI) of the Freedom Online Coalition (FOC) is instructive for understanding the rights that are most invaded in the digital space, such as the right to privacy, non-discrimination, freedom of opinion and expression. The preamble is building on the Human Rights Council (HRC) Resolution from 2012 confirming that international human rights law and international humanitarian law apply online and well as offline. It reiterates that cybersecurity must protect both technological innovation and the exercise of human rights. The Initiative uses the following definition to reflect the belief that respecting human rights should be a central part of

cybersecurity and cybersecurity-related policymaking: Cybersecurity is the preservation – through the law, 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 (*as defined by International Organization for Standardization (ISO) 27000 standard) (FOC 2015, 1). This definition promotes cybersecurity as a concept which recognises basic rights and fundamental freedoms as its core components.

2. The Human Rights Dimension of Cybersecurity

The same technologies and platforms that were hoped to serve as a forum for democratic processes, connect people across the globe, and provide for greater security have exposed citizens to an unprecedented attack on their fundamental rights. The expansion of sophistication and extent of internet censorship and mass surveillance by state actors can be taken as an example to illustrate why the use of such practices invigorates debates about the balance between security and human rights. Cybersecurity practices that clash with individual freedoms have been particularly visible in the instances of governments reacting to terrorist threats (Commissioner for Human Rights 2016) or recently with the countering measures limiting the spread of COVID-19 (AccessNow 2020a; Fildes and Espinoza 2020 Yang at el. 2020). China, Israel, South Korea, the United States, and other governments introduced contact tracing or used geolocation and proximity information from mobile phones with a goal of slowing the spread of the virus (Human Rights Watch 2020b). European countries alike authorised governmental agencies to use data from telecoms companies for ensuring that infected people stay in quarantine (Shotter 2020). Human Rights Watch has cautioned about the deployment of mobile location tracking programs used by governments in the fight against the virus, raising concerns about *'unnecessary and disproportionate surveillance measures in public health disguise'*. It also warned that unproven and untested technologies can pose serious risks to human rights with severe threats to security arising in countries with experiences in intrusive surveillance practices, where they have a potential of being misused for monitoring, tracking and repression (Human Rights Watch 2020b).

The cybersecurity discourse around these issues is predominantly shaped by the concept of national security that places civil liberties and human rights under devaluating pressure or even positions them as antithetical to national security in a zero-sum game (Hildebrandt 2013, 14; Pagallo 2013,

390-391). Human rights are discussed as part of the framework but the prevailing understanding of what constitutes cybersecurity remains heavily focused on the level of sovereign state – its territory and its infrastructure – rather than the individual. This phenomenon can be understood from an international relations perspective as a realpolitik approach to governance when state interests are privileged, and a military-centric approach to the issue prevails. While these perceptions differ depending on the country and regional context, the realist cybersecurity view has been dominant in the cybersecurity decision-making. This view is to some extent justified, as security is a precondition to the enjoyment of human rights but does not place an equal emphasis on human rights as a precondition to security. For this reason, it remains insufficient for addressing the needs of individuals, especially those with high cybersecurity risks. To address these gap, Association for Progressive Communications (APC 2020) defines a human rights-based approach to cybersecurity as *'putting people at the centre and ensuring that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Such an approach is systematic, meaning that it addresses the technological, social and legal aspects together, and does not differentiate between national security interests and the security of the global internet*'.

The human rights centric approach goes beyond protection of electronic data and the military understanding of security as securing cyberspace and related critical infrastructure of states from external threats. It does so by shifting the focus to people's security and human rights, and importantly on how their possible violations turn citizens from technological beneficiaries to victims. More than that, it empowers them to the full enjoyment of their rights. This approach can be also understood through a positive and negative view of security. The negative way understands security as the absence of threats to core human values, while the other promotes the understanding of security as the policies and practices that safeguard and enable people to exercise their rights freely and securely (Liaropoulos 2015, 19). In accordance with this view, Kovacs and Hawtin (2013, 7) state that cybersecurity should not merely play a defensive role, but a facilitating role, by effectively putting the empowerment and well-being of people at the centre. These approaches are best suited for the new challenges introduced by cyberspace. Firstly, they help to understand how human rights and security are interrelated and interconnected. Secondly, they reflect on the growing importance of the ICTs in people's lives and consequently their reliance on them, and by doing so, they help to address the fading divide between the online and offline world. The question of whether, and to what extent, it is necessary to curtail civil liberties and human rights in order to combat security threats should

be hence guided by the principles that take national security as means to provide the citizens with a secure environment.

3. Human Rights and International Cooperation in Cyberspace

Human rights are rights guaranteed under the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Their online implementation has been primarily addressed by the HRC in the resolution on the promotion, protection and enjoyment of human rights on the Internet adopted in 2012. The Council concluded that *'the same rights that people have offline must also be protected online'* (UN Human Rights Council 2012). The Council later called on the states to *'address security concerns on the Internet in accordance with their international human rights obligations to ensure the protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet'* (UN Human Rights Council 2016). Yet, translating the international human rights standards inro practical realms of cyberspace has proven difficult.

One of the most battled principles connected to the cyberworld is the right to privacy, which has a direct link to the security of people. HRDs, journalists, activists, and other groups can be particularly at risk of intercepted communications, hacked accounts, phishing campaigns, excessive data collection or electronic surveillance. Hildebrandt (2013, 2) proposes to understand this complex right as *'the freedom from unreasonable constraints on identity construction, while taking into account that a number of other fundamental rights are at stake, notably data protection, non-discrimination, due process and free speech*'. This statement illustrates that the right to privacy is instrumental in exercising a range of individual and political rights. The right to privacy is included in Article 12 of the *Universal Declaration of Human Rights* (UN 1948) and Article 17 of the *International Covenant on Civil and Political Rights* (UN 1966), but its wording is limited to the prohibition of arbitrary or unlawful interference with one's privacy and the right for protection of the law against such interference or attacks. The international community led by HRC, UN special rapporteurs, and related state and non-state actors have worked towards overcoming the absence of a more comprehensive framework, including issues around digital privacy (UN 2019), but the position provides for different interpretations. In the

result, while governments have obligations to respect and protect the right to privacy and to ensure that everyone can enjoy it, the lack of clarity on its potential restrictions legitimises some of the methods that limit exercising this right fully.

New technologies present a particular threat to this right. Electronic surveillance, mass information collection and biometric identification are just some of the technologies which have a potential of being used against targeted individuals or communities, including HRDs, dissent, journalists, minorities or marginalised groups. Given their use in public offline and online space, expanding capacities, the use of AI, and the general secrecy and the lack of oversight when deployed by state actors, they pose new and unprecedented challenges for exercising rights and freedoms and can introduce additional risks for the safety and security of people.

Citizens have reduced privacy expectations in public (Madden and Rainie 2015), but the right to privacy nevertheless exists in public spaces and is protected by national and international instruments to varying degrees both by national and international instruments, including the widely ratified *ICCPR* (Naef 2020). Privacy rights can be infringed only within strict limitations under most international human rights instruments. Some form of surveillance can be present under specific circumstances. For instance, the *European Convention on Human Rights* (ECHR 2003) includes provisions for the rights to privacy in Article 8 stating that interference with the right by a public authority can only occur if '*it is in accordance with the law*; and, *necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'*. Technology tools can play an important role in efforts to save lives, for instance by spreading public health messages and increasing access to health care such as was the case of some coronavirus countering measures. But beyond proportionality, the short-term emergency solutions bring a danger of keeping methods prone to abuse at state's disposal interminably (ICJ 2020).

Over the past years, concerns about human rights violations in cyberspace have been addressed on both the international and national level. At the international level, the Group of Governmental Experts (GGEs) and the Open-ended Working Group have been appointed by the UN General Assembly to discuss responsible state behaviour in cyberspace and to report on the nature of cyber threats and their consequences for national and international security. The reports issue by GGEs underscored that states have to respect human rights and fundamental freedoms when addressing cybersecurity issues (Rossini and Green 2015). UN Human Rights Council's

Special Procedures, comprising of independent human rights experts with mandates to report and advise on human rights from a thematic or country-specific perspective, also submitted a number of reports on the issue of surveillance, encryption and anonymity (UN Special Rapporteur, 2018; UN Special Rapporteur 2019).

The Organisation of Security and Co-operation in Europe (OSCE) and the European Union (EU) have also adopted principles or tasked member states to build collaboration around cybersecurity issues and the applicability of international law including human rights law to cybersecurity. In the 2016 Ministerial Decision (OSCE 2016), OSCE participating States decided to step up individual and collective efforts to address the security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments including responsibilities to respect human rights and fundamental freedoms (OSCE 2016). In 2013, the EU issued its first Cyber Security Strategy (European Commission 2013, 5, 15), in which it outlined the aim to create a *'coherent international cyberspace policy'* where it could promote core values such as *'human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights'*. A number of other EU bodies was tasked to provide further assistance, information sharing, and training to the member states (Barrinha and Renard 2020). It also tasked the member states to build collaboration around cybersecurity issues and the applicability of international law including human rights law to cybersecurity (Rossini and Green 2015).

These are important achievements on the way to the respect of human rights in cyberspace, but they often lack commitment on the national level and consequently implementation on the ground. To address this gap, a number of international initiatives have been calling for an overhaul of the current cybersecurity policies and practices, notably the Freedom Online Coalition (FOC) – a partnership of governments working to advance Internet freedom. FOC coordinates ad hoc Working Groups that provide a mechanism for focused and issue-based engagement as well as provide an avenue for multi-stakeholder engagement with the participating governments. In 2016, FOC launched policy recommendations for human rights-based approaches to cybersecurity, which preamble reads that 'these recommendations 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' (FOC 2016). Initiatives on both the institutional and the civil society spectrum of cybersecurity stakeholders contribute to the discussion, often through reporting on violations of human rights or building capacity on these issues

among citizens, including manuals and training for HRDs to implement tactics and tools for digital security (Front Line Defenders no date; Nyst 2016; OSCE/ODIHR 2019; OSCE/ODIHR 2020).

4. Threats to HRDs' Security

The security risk in cyberspace is higher for targeted groups, in particular HRDs, but also journalists, activists, marginalised and discriminated groups. If their channels of communication, access to information and storing of information are not secure, it can lead not only to their compromised digital security, but as well to psychosocial insecurity, and in extreme cases, to risks to their personal physical security and security of their connections who are often vulnerable cases such as victims of crimes or minorities. Examples of such risks include government hacking, data breaches, Internet shutdowns, distributed denial of service (DDoS) attacks, targeted malware and ransomware, phishing and limiting the use of encryption and anonymity-enhancing technologies, which happens both on the legal level through proposals to introduce backdoors access to the encrypted conversations and in practical terms when these communications are compromised, blocked or disabled to access (APC 2020).

The use of computers, smartphones, social media platforms, messaging apps, and other technological tools and solutions have become indispensable to HRDs work, communication and activism. While this allows for more efficient use of resources, easier communication and a greater advocacy reach, it also adds to the list of potential vulnerabilities (Higson-Smith et al. 2016, 11-13). This trend has been reinforced during the COVID-19 pandemic when many HRDs who have previously conducted interviews and meetings in person, had to transition into the online realm which has increased their reliance on digital channels of communication. The same applies to their information, such as content and contacts, which have been increasingly transformed into digital form. The related weaknesses are connected to the fact that data can be stored, accessed, processed, mined by third parties and hence reveal sensitive information. Risks comprise of manual access to the data and accounts, such as data loss, information handover compromised accounts, device confiscation, theft or inspection as well as technologically empowered interference including tracking, phishing and targeted malware (Higson-Smith et al. 2016, 73-74). Additional risks stem from the possible access to the metadata which many of them produce without their knowledge and without the needed caution about their digital footprint. The Internet Protocol (IP) address, location data, the unique identifying numbers of the

SIM card and the phone, the senders, recipients, timestamps and subjects of emails, and whether they include attachments, properties of image files or documents – these are some of the metadata that can be misused for tracking and monitoring.

The physical threats remain among HRDs biggest concerns – stolen hard drives, searched files are targeted attacks often initiated by actors whose misconduct they are trying to investigate (Notley and Hankey 2013, 161-162). These cases usually go unreported and unpublished, and unless the information is further distributed or 'leaked' for the purpose of discreditation, it is difficult to prove the motive. For instance, Frontline Defenders reported that unknown individuals raided the home of indigenous woman human rights defender in November 2019. Personal documents, phones and digital files were taken, while valuable objects were left behind (Front Line Defenders 2019). A popular method to attack HRDs related to their information is phishing – the fraudulent practice of sending emails purporting to be from reputable senders in order to induce individuals to reveal personal information. These are especially common in countries where there is a low risk of searches and seizures. Digital Security Lab Ukraine reported a phishing campaign against several prominent Ukrainian HRDs and journalists, alerting that *'campaign includes emails posing as Facebook alerts, leading to different phishing domains'* (Digital Security Lab 2019). Amnesty International investigation revealed several similar attacks, including a campaign of malicious emails in Uzbekistan between May and August 2019 (Amnesty International 2020d), and a series of broad phishing campaigns targeting HRDs, journalists, political actors and others in many countries throughout the Middle East and North Africa region around 2019 (Amnesty International 2020e). Later investigation has found that a wave of digital attacks starting from January 2019 likely originated from government-backed bodies and involved multiple attempts to gain access to the email accounts of several prominent Egyptian HRDs, media and civil society organizations' staff (Amnesty International 2020c). Amnesty International together with the Citizen Lab also uncovered a coordinated spyware campaign targeting several HRDs in India, among which a common link was that they have been calling for the release of other prominent activists. Between January and October 2019, the HRDs were targeted with emails containing malicious links, which included spyware able to compromise the computers and monitor their actions and communications (Amnesty International 2020b). Such interception of communications and compromise of the confidentiality of information violates the right to privacy and the right to freedom of expression, among other rights.

It was anticipated that in countries with a track record of censorship practices, the online space, and notably social media, could become a substitute for the public sphere, empowering people to freely access information, communicate and express their opinions. But with the governments adopting increasingly sophisticated technology, possibilities for voicing opposition are diminishing. The denial of availability of information and its underlying infrastructure violates a wide range of fundamental rights, including by disproportionately restricting access to information and limiting the ability of people to express themselves, peacefully assemble and associate, as well as they violate economic, social and cultural rights (APC 2020).

Internet censorship, blocking and filtering of online activities under security pretexts have been used by a number of governments. An extreme example of censored and policed Internet is the Great Firewall of China – a massive mechanism of censorship and surveillance that enables restricting content, identifying and locating individuals, and providing immediate access to personal data. Back when it was established in 2001, the Firewall blocked only several websites identified as those that disseminate 'subversive' information, and importantly, it was possible to circumvent the blockage. Gradually more websites have been blocked since then, and further legal and technological obstacles have been put to prevent bypassing the digital censorship system (Maranto 2020; Wang 2020), such as banning the use of unapproved Virtual Private Networks (VPNs) that effectively restricted users from accessing online information outside the country (Solon 2017). This case is a strong demonstration of how an overemphasis on realpolitik and the national security view uses 'sovereignty' to not only justify violations of human rights but also preclude international observers from pointing to these violations. Its accent on control and centralization as opposed to genuine concern for individual security makes people more vulnerable and allows for an unprecedented control tying their online behaviour to a 'social credit' system ranking their reliability as citizens (Deibert 2018, 418).

Chinese authorities' approach to the internet based on control and increasing isolation and is not a solitary attempt to push for fragmentation of the global internet. Russia has also significantly expanded laws and regulations tightening control over internet infrastructure, online content, and the privacy of communications (Polyakova and Meserole, 6-11). In November 2019, President Vladimir Putin introduced new regulations that create a legal framework for centralised state management of the internet within Russia's territory. It allows the authorities to block access to the internet without judicial oversight, in the event of undefined security threats (Human Rights Watch 2019). If implemented, this framework will lead to centralized control of the country's internet traffic, censorship and greater

control over society which will severely undermine the ability to exercise human rights online, including freedom of expression and freedom of access to information (Human Rights Watch 2020c). China and Russia have formally endorsed legal principles concerning appropriate conduct in cyberspace, but as demonstrated it routinely violate them in practice (Deibert 2018, 413).

Many other countries opt for repressive measures during times of elections, protests or emergencies. Internet shutdowns, also called "network shutdowns", "kill switches" or "blackouts", are a particularly pernicious way of interfering with communication technologies and platforms and thus also with assemblies. UN Human Rights Council recorded at least 65 Internet shutdowns which took place during protests in 2019, jeopardizing the right of peaceful assembly both online and offline (UN Human Rights Council, 2020) Notably, they are becoming increasingly common in some African countries, most recently Tanzania during the elections in October 2020, Ethiopia in response to unrest in June 2020, and Zimbabwe, Togo, Burundi, Chad, Mali and Guinea during some point during the year (Giles and Mwai 2020).

A closely watched incident took place also in Europe when the Belarussian government shut down access to much of the internet to prevent people from expressing their discontent with the result of the presidential elections in August 2020 (Netblock 2020).

Internet shutdowns and blocked social media platforms are increasingly popular as a method of curbing the discontent and preventing communication and coordination of protests. Such methods are particularly dangerous in times of emergencies, as HRDs and journalists are unable to speak with their sources and informants, continue their monitoring, and verify the footage posted online. As alternative sources of communication such as mobile phone calls are highly insecure due to governmental control, they conduct their work in a high-risk environment with possibly dire consequences for their personal security (AccessNow 2020b, 15). Strong end-to-end encryption messaging platforms which are able to work despite the government interference have proven to be of high importance in such cases (Human Rights Watch 2020a). Encryption is also an enabler of enjoying the rights to freedom of expression, information and opinion, with an impact on the rights to freedom of peaceful assembly, association and other human rights (Amnesty International 2016). The 2017 resolution of the UN Human Rights Council, noting that good practices aimed at protection of HRDs and those of journalists should be, where applicable, be relevant inter alia, emphasised that *"in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy,*

including to secure their communications and to protect the confidentiality of their sources" and called upon States *"not to interfere with the use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law"* (UN General Assembly 2017, 3, 6 par 14). Together with anonymity tools, pseudonyms, and other digital security features encryption empowers individuals to operate in a safe digital space and is essential to defend against unlawful access to data and to protect users, especially communities at greater risk of unwarranted surveillance (AccessNow 2020b, 24).

New technologies are a distinct category presenting threats to HRDs security. Electronic surveillance, coupled with facial recognition software, data collection and profiling, and biometrics identification are examples of rapidly developing technologies used primarily for national security purposes, but they can be just as easily used for generating, collecting and storing data on any groups or individuals. Under the mandate of countering terrorism, protecting public order, deterring common crimes, increasing border security or road safety, states can weaponize cybersecurity-related protection to exercise stricter control over their citizens, and target the surveillance measure to principally include their opposition and critics. Electronic surveillance and data collection practices are less obvious in their direct impact on the work of HRDs than the above-mentioned practices but because of their 'chilling' effect, they lead to people's inclination to self-censorship of their behaviour and expression and this way have a negative impact on their rights, in particular the freedom of expression and the right of assembly (Penney 2017; FRA 2019, 4). More evidence showing the use of collected data against the work of HRDs need to be investigated, but cases of abuse of their rights, misconduct of the authorities using them, general misuse and lack of safeguards accompanying deployment of such technologies, and possible implications for human rights have been raised in great detail.

With growing capacity and sophistication of technological solutions, states have increased and enhanced monitoring and control measures. This is also traceable in the use of electronic surveillance employing facial recognition technology. The smart city model popularised in the past decade is a fitting example. While many countries have adopted smart cities technologies to optimise infrastructure, mobility and the use of public services, some of them heavily focused on the national security aspect and incorporated a centralised system combining facial recognition cameras and various sensors (Jardine 2019). Chinese and Russian firms are among the chief producers and exporters of advanced surveillance technology globally. Common export destinations are countries in Central Asia and South America (Feldstein

2019; Mozur 2020; Yan 2019). The countries' track record of monitoring their citizens and suppressing opposition is a warning sign, especially taking into consideration that already having such solutions in place can lead to states being more prone to monitor certain groups of population or individuals (Naef 2020). Should such technologies be deliberately used for surveillance purposes, they can enable for tracking HRDs information, conversations and actions to the point of making them unable to operate.

Some other countries are prone to expanding the use by new technologies by security, military and law enforcement agencies. This aspect is particularly problematic as these bodies operate in a secretive environment. While their advocates emphases their efficiency and priciness, they can lead to indiscriminate surveillance if they are not accompanied by adequate countervailing measures. The practise as well as the capacity of new technologies increase while the accompanying legislation, regulation and oversight lag behind (UN Special Rapporteur 2019). Several temporary bans on the use of facial recognition technologies have been introduced on the national and local level, temporarily postponing their deployment until the legislative and regulatory frameworks catch up with the technological developments. Some US cities have banned the state agencies from using facial recognition technologies pointing to faults in their algorithms (Commonwealth of Massachusetts 2020; Conger at al. 2019; Hill 2020; Holmes 2020). Social movements and campaigns for a ban and upholding human rights have culminated during protests over police brutality and racial discrimination in the United States in summer 2020 (ACLU 2020; Amnesty International 2020a Devich-Cyril 2020). As a result of the growing public scrutiny, a number of companies working on facial recognition technologies, including Amazon, IBM and Microsoft, announced they would limit or halt their sales to law enforcement agencies citing concerns over mass surveillance and racial profiling (BBC 2020a; BBC 2020b). The pressure is also rising on EU decision-makers to regulate facial recognition in public space as a part of the expected release of AI laws which are under preparation (Reventlow and Chander 2020).

Use of these technologies increases the insecurity mindset among HRDs and other targeted and non-conformist groups. It can also violate a wide range of human rights – primarily the right to privacy, and consequently the right to freedom of opinion and expression, peaceful assembly and freedom of association. The decision-making on facial recognition and other AI-powered new technologies needs to take into account the viewpoints of individuals and communities whose rights are at high risk of being violated and use their cases studies for drawing limits the red lines. Prior to the deployment, authorities should conduct human rights impact assessments

and ensure that their use is proportional, transparent and accompanied by a system of checks and balances (EDRi 2019).

5. Recommendations: Legislation, Oversight and Capacity Building

With the increasing use of technologies, we stand in front of an uneasy task of translating the established values and principles into the cyber realm. The human-centred dimension of cybersecurity has been absent in the current narrative, and consequently decision-making and practices which remain heavily influenced by the realpolitik view of protecting only national security. However, cybersecurity is just as much about preventing attacks of the vital services as it is about protecting individual users. The outlined cases of compromised security for vulnerable groups demonstrate that the current cybersecurity framework falls short on protecting the full enjoyment of human rights. To address this gap, policies and procedures should take into consideration the disproportionate threats faced by individuals and groups at risk. Approached from the lenses of positive security, cybersecurity laws, norms and practices should enhance the security of persons both online and offline. To this goal, they should guarantee protection for fundamental rights, and the right to privacy in particular, as preeminent with respect to the enjoyment of other rights.

The norms and the protocols of the cyberspace were in large developed independently of the state – as a result, much of the infrastructure and services are owned by the private sector, and the Internet users operate across jurisdictions. However, states remain the most powerful actors in cyberspace with the legal obligation to protect and promote human rights. The state agencies are also essential to enforce the rule of law in order to protect the rights of their citizens. But the legislative frameworks have been lacking behind the technological developments and did not proactively mitigate the risks, or often, as outlined above, even used against the people. The legal framework needs to be supported by the norms guiding our societies. In principle, international human rights norms do provide an overall framework, but implementation remains problematic. The legal framework for cybersecurity is challenging not only due to the transnational nature of issues, competing visions, and fast technological developments, but also as a result of multiple players. In particular, private companies in this domain have acquired power and resources which can compete with those of many sovereign countries. They also have been placed or often even positioned themselves outside of the existing legal framework. To the

goal of developing comprehensive policies, governmental and international bodies need to work toward creating a transparent and accessible multi-stakeholder environment, which includes a vast array of stakeholders, including civil society representatives (FOC 2015). Starting at the point of human-rights centric policy creates an environment supporting cooperation and innovation and places the emphasis on the common grounds when setting international standards.

Effective international and national oversight and transparency are key for ensuring that the norms and legislation agreed behind a table are complied with in practice. On the level of the state, the scrutiny should be put over the delegated bodies which deal with cybersecurity, including military, intelligence and law enforcement agencies which operate with limited oversight, transparency and hence public accountability (Deiber 2018, 411). As proved by the Snowden revelations, liberal democracies are not an exception from misusing the national state apparatus in line with a realpolitik national security approach. While certain limitations to fundamental rights in times of emergency can be applicable, they must be justified with a legitimate aim, tailor-made to ensure proportionality, time-bound to the necessary period and accompanied by adequate and effective safeguards (Hildebrand 2013, 2). The second layer of an independent oversight must be placed on the private actors – both on the cross-cutting issue of development, supply and deployment of their technological solutions to state agencies, and on how they use technologies to expand their business models.

Together with existing international standards, international organisation and courts provide important interpretations of human rights into practice. Experts from the United Nations, OSCE, Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR) have declared that internet shutdowns cannot be justified under international human rights law (AccessNow 2015). The European Court of Human Rights (ECHR) have issued important decisions such as that the overbroad restrictions or blocking orders that inhibit access to entire web services or domains cannot be held to be proportionate restrictions to internationally protected fundamental rights under international human rights law. These critical court decisions reiterate that states cannot justify restricting access to information (AccessNow 2019), which has been misused especially during periods of social unrest and protest.

The human-centric approach to cybersecurity should be supported by growing cybersecurity awareness in the society to the goal of creating a level playing field. The more citizens find this field approachable the more it will enhance the multi-stakeholder decision-making as well as public oversight. Special emphasis should be placed on the specific needs of targeted groups

which face higher security risks. Capacity building programmes that build technological awareness and teach proactive ways of protecting information can be vital for mitigating the negative consequences of deficiencies in the current cybersecurity framework. These efforts need to be supported by technologies which have human-rights centred security in their core, and which overarching principle is to build solutions which serve the society. Privacy and security-enhancing technologies are essential enablers of human rights. End-to-end encryption, pseudonyms, and anonymity features empower individuals to connect, gather information and mobilize without the fear of excessive access to data, unwarranted surveillance and other forms of interference and ensure that people regain control over their devices.

Conclusion

There has been a prevailing understanding of what constitutes cybersecurity based on national security. But with the lines between offline and online world gradually disappearing, this view falls short on addressing the pressing issue of what cybersecurity means for individual users. The urgency of this issue is demonstrated on cases studies of HRDs which are among the targeted groups in cyberspace. As countries continue violating freedoms of their citizens under the pretext of national security, it is vital that we are guided by a narrative which does not be position human rights against national security, neither devalues them as a part of the trade-off.

At the core of any security policy should be the initial question of what is being secured and the decision-making and policymaking follow the set of guiding principles and objectives. The human-centric approach focuses on the security of the citizen which is often overlooked. Starting at the point of the human-rights centric policy is the way how to refocus this discussion to create an environment for a more collaborative way to security (Deibert 2018, 419-420). While this approach challenges the prevailing understanding of national security as a matter of exclusively national security, its aim is to be complementary rather than to compete. Striking the right balance between them is a precondition for providing security which allows the citizens to exercise human rights.

Bibliography

AccessNow, (2015) 'Internet kill switches are a violation of human rights law, declare major UN and rights experts', retrieved from: https://www.

accessnow.org/internet-kill-switches-are-a-violation-of-human-rights-law-declare-major-un/ (accessed 30/11/2020).

AccessNow, (2019) '#KeepItOn: Keeping the internet open and secure in Hong Kong', retrieved from: https://www.accessnow.org/keeping-internet-open-in-hong-kong/ (accessed 30/11/2020).

AccessNow, (2020a) 'Access Now joins 100+ organisations in telling governments: don't use the coronavirus pandemic as cover for expanding digital surveillance', retrieved from: https://www.accessnow.org/access-now-joins-100-organisations-in-telling-governments-dont-use-the-coronavirus-pandemic-as-cover-for-expanding-digital-surveillance/ (accessed 30/11/2020).

AccessNow, (2020b) 'Defending peaceful assembly and association in the digital age takedowns, shutdowns, and surveillance', retrieved from: https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf (accessed 30/11/2020).

ACLU, (2020) 'How is Face Recognition Surveillance Technology Racist?' retrieved from: https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/ (accessed 30/11/2020).

Amnesty International, (2016) 'Encryption: A Matter of Human Rights', retrieved from: https://www.amnesty.org/download/Documents/POL4036822016ENGLISH.pdf (accessed 30/11/2020).

Amnesty International, (2020a) 'Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance', retrieved from: https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/ (accessed 30/11/2020).

Amnesty International, (2020b) 'India: Human Rights Defenders Targeted by a Coordinated Spyware Operation', retrieved from: https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/. (accessed 30/11/2020).

Amnesty International, (2020c) 'Phishing attacks using third-party applications against Egyptian civil society organizations', retrieved from: https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/ (accessed 30/11/2020).

Amnesty International, (2020d) 'Uzbekistan: New Campaign of Phishing and Spyware Attacks Targeting Human Rights Defenders', retrieved from:

https://www.amnesty.org/en/latest/news/2020/03/uzbekistan-new-campaign-of-phishing-and-spyware-attacks-targeting-human-rights-defenders/ (accessed 30/11/2020).

Amnesty International, (2020d) 'When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users,' retrieved from: https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/ (accessed 30/11/2020).

APC, (2019) 'Why cybersecurity is a human rights issue, and it is time to start treating it like one', retrieved from: https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one (accessed 30/11/2020).

APC, (2020) 'APC policy explainer: A human rights-based approach to cybersecurity', retrieved from: https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity (accessed 30/11/2020).

Barrinha, A.,Renard, T., (2020) 'The EU's International Politics of Cyberspace in an Emerging Post-Liberal Order', *Friends of Europe*, retrieved from: www.friendsofeurope.org/insights/the-eus-international-politics-of-cyberspace-in-an-emerging-post-liberal-order (accessed 30/11/2020).

BBC, (2016) 'The Vocabularist: How we use the word cyber', retrieved from: https://www.bbc.com/news/magazine-35765276 (accessed 30/11/2020).

BBC, (2020a) 'George Floyd: Amazon bans police use of facial recognition tech', retrieved from: https://www.bbc.com/news/business-52989128 (accessed 30/11/2020).

BBC, (2020b) "George Floyd: Microsoft bars facial recognition sales to police', retrieved from: https://www.bbc.com/news/business-53015468 (accessed 30/11/2020).

Commissioner for Human Rights, (2016) 'Human rights in Europe should not buckle under mass surveillance.' *Council of Europe Portal*, retrieved from: https://www.coe.int/en/web/commissioner/-/human-rights-in-europe-should-not-buckle-under-mass-surveillance (accessed 30/11/2020).

Commonwealth of Massachusetts, (2020) 'An Act establishing a moratorium on face recognition and other remote biometric surveillance systems. Bill S.1385.' retrieved from: https://malegislature.gov/Bills/191/SD671 (accessed 30/11/2020).

Conger, K., Fausset, R., Kovaleski, S. F. (2019) 'San Francisco Bans Facial Recognition Technology', *New York Times*, retrieved from: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (accessed 30/11/2020).

Deibert, R. J. (2018) 'Toward a Human-Centric Approach to Cybersecurity', *Ethics & International Affairs* 32 (4), 411–424, doi:10.1017/S0892679418000618.

Devich-Cyril, M. (2020), 'Defund Facial Recognition', *The Atlantic,* retrieved from:

https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ (accessed 30/11/2020).

Digital Security Lab Ukraine, (2019) 'We are tracking an active targeted phishing campaign…,' *Twitter,* retrieved from: https://twitter.com/DSLab_Ukraine/status/1174335634141569024?s=20 (accessed 30/11/2020).

ECHR, (2003) 'European Convention on human rights. Act number 20 of 2003,' retrieved from: https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed 30/11/2020).

EDRi, (2019) 'Facial recognition and fundamental rights 101,' retrieved from: https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/ (accessed 30/11/2020).

European Commission, (2013) 'EU Cyber Security strategy: An open, safe and secure Cyberspace,' retrieved from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf (accessed 30/11/2020).

European Union Agency for Fundamental Rights (FRA), (2019) 'Facial recognition technology: fundamental rights considerations in the context of law enforcement,' retrieved from: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (accessed 30/11/2020).

Feldstein, S. (2019) 'The Global Expansion of AI Surveillance,' *Carnegie Endowment for International Peace,* retrieved from: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (accessed 30/11/2020).

Fildes, N., Javier, E., (2020) 'Tracking coronavirus: big data and the challenge to privacy', *Financial Times*, retrieved from: https://www.

ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987 (accessed 30/11/2020).

Freedom Online Coalition (FOC), (2015) 'Recommendations for Human Rights based approached to cybersecurity,' *Working Group 1 "An Internet Free and Secure"*, retrieved from: https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf (accessed 30/11/2020).

Freedom Online Coalition (FOC), (2019) 'WG1 launches recommendations on human rights-based approaches to cybersecurity', retrieved from: https://freeandsecure.online (accessed 30/11/2020).

Front Line Defenders, (2019) 'Raid on House of Indigenous Rights Defender Alessandra Korap', retrieved from: https://www.frontlinedefenders.org/en/case/raid-house-indigenous-rights-defender-alessandra-korap (accessed 30/11/2020).

Front Line Defenders, (no date) 'Security in A Box - Digital Security Tools and Tactics', retrieved from: https://securityinabox.org/en/ (accessed 30/11/2020).

Giles, C., Mwai, P, (2020) 'Africa internet: Where and how are governments blocking it?' *BBC*, retrieved from: https://www.bbc.com/news/world-africa-47734843 (accessed 30/11/2020).

Higson-Smith, C., Cluanaigh D. O., Ravi, A. G. Steudtner, P. et al. (2016) 'Holistic Security: A Strategy Manual for Human Rights Defenders,' retrieved from: https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/62/hs_complete_lores.pdf (accessed 30/11/2020).

Hildebrandt, M. "Balance or Trade-off? Online Security Technologies and Fundamental Rights." *Philosophy & Technology* 26 (4),357–379, doi:10.1007/s13347-013-0104-0.

Hill, K. (2020). 'Activists Turn Facial Recognition Tools Against the Police', *New Your Times,* retrieved from: https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html (accessed 30/11/2020).

Holmes, A. (2020) 'Boston just became the latest city to ban use of facial recognition technology', *Business Insider*, retrieved from: https://www.businessinsider.com/boston-bans-government-use-of-facial-recognition-technology-2020-6 (accessed 30/11/2020).

Human Rights Watch, (2020a) 'Belarus: Internet Disruptions, Online Censorship', retrieved from: https://www.hrw.org/news/2020/08/28/belarus-internet-disruptions-online-censorship (accessed 30/11/2020).

Human Rights Watch, (2020b) 'Covid-19 Apps Pose Serious Human Rights Risks: Recommendations for Governments Considering Technology in Addressing Pandemic', retrieved from: https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks (accessed 30/11/2020).

Human Rights Watch, (2020c) 'Russia: Events of 2019', retrieved from: https://www.hrw.org/world-report/2020/country-chapters/russia (accessed 30/11/2020).

International Commission of Jurists (ICJ), (2020) 'Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights', retrieved from: https://www.icj.org/wp-content/uploads/2020/04/COVID-19-Surveillance-Joint-Statement-2020-ENG.pdf (accessed 30/11/2020).

Jardine, B. (2019) 'China's Surveillance State Has Eyes on Central Asia,' *Foreign Policy*, retrieved from: https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/ (accessed 30/11/2020).

Kovacs, A., Hawtin, D. (2013) 'Cyber Security, Cyber Surveillance and Online Human Rights', *Global Partners Digital*, retrieved from: https://www.gp-digital.org/wp-content/uploads/2013/05/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf (accessed 30/11/2020).

Liaropoulos, A. (2015) 'A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia,' *Journal of Information Warfare* 14 (4), 15–24.

Madden, M., Rainie L. (2015) 'Americans' Attitudes About Privacy, Security and Surveillance', *Pew Research Center: Internet, Science & Tech*, retrieved from: www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (accessed 30/11/2020).

Maranto, L. (2020) 'Who Benefits from China's Cybersecurity Laws?' *The Center for Strategic and International Studies (CSIS)*, retrieved from: https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws (accessed 30/11/2020).

Mozur, P, Kessel, J. M., Chan, M. (2019) 'Made in China, Exported to the World: The Surveillance State', *New York Times* retrieved from: https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html (accessed 30/11/2020).

Naef, B. (2020) 'Taming State Surveillance: Reconciling Camera Surveillance Technology with Human Rights Obligations', *HillNotes* retrieved from: www.hillnotes.ca/2020/03/16/taming-state-surveillance-reconciling-camera-surveillance-technology-with-human-rights-obligations (accessed 30/11/2020).

NetBlocks, (2020) 'Internet disruption hits Belarus on election day', retrieved from: https://netblocks.org/reports/internet-disruption-hits-belarus-on-election-day-YAE2jKB3 (accessed 30/11/2020).

Notley, T., Hankey, S. (2013) 'Human Rights Defenders and the Right to Digital Privacy and Security,' in: Lannon, J., Halpin. E. F. (eds.) *Human Rights and Information Communication Technologies: Trends and Consequences of Use,* IGI Global, 157-175, doi:10.4018/978-1-4666-6433-3.ch108.

Nyst, C. (2016) 'Travel Guide to the Digital World: Cybersecurity Policy for Human Rights Defenders', *Global Partners Digital* retrieved from: https://www.gp-digital.org/wp-content/uploads/2016/05/Travel-Guide-to-the-Digital-World_Cybersecurity-Policy-for-HRD.pdf (accessed 30/11/2020).

OSCE Permanent Council, (2016) 'Decision No. 1202 OSCE Confidence-building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies', retrieved from: https://www.osce.org/files/f/documents/d/a/227281.pdf (accessed 30/11/2020).

OSCE/ODIHR, (2019) 'Open Source Human Rights Monitoring Training,' retrieved from: https://www.osce.org/odihr/420107 (accessed 30/11/2020).

OSCE/ODIHR, (2020) 'Call for applications: ODIHR Training on Open Source Human Rights Monitoring,' retrieved from: https://www.osce.org/odihr/training-human-rights-monitoring (accessed 30/11/2020).

Ottis, R., Peeter, L. (2011) 'Cyberspace: Definition and implications,' *5th European Conference on Information Management and Evaluation (ECIME),* 267-270. retrieved from: https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf (accessed 30/11/2020).

Pagallo, U. (2013) 'Online Security and the Protection of Civil Rights: A Legal Overview," *Philosophy & Technology* 26 (4), 381–395, https://doi.org/10.1007/s13347-013-0119-6.

Penney, J.W. (2017) 'Internet surveillance, regulation, and chilling effects online: a comparative case study', Internet Policy Review 6 (2), doi:10.14763/2017.2.692.

Polyakova, A., Meserole, C. (2020) 'Exporting digital authoritarianism: The Russian and Chinese models', *Foreign Policy at Brookings*, retrieved from: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf (accessed 30/11/2020).

Reventlow, N. J., Chander, S. (2020) 'US Corporations are talking about bans for AI. Will the EU?' *EURACTIVE,* retrieved from: https://www.euractiv.com/section/digital/opinion/us-corporations-are-talking-about-bans-for-ai-will-the-eu/ (accessed 30/11/2020).

Rossini, C., Green, N. (2015) 'Cybersecurity and Human Rights." *Public Knowledge*. retrieved from: https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf. (accessed 30/11/2020).

Rout, D. (2015) 'Developing a Common Understanding of Cybersecurity', *ISACE Journal* 6, retrieved from: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/developing-a-common-understanding-of-cybersecurity (accessed 30/11/2020).

Shotter, J. (2020) 'Slovakia to track coronavirus victims through telecoms data." *Financial Times*, retrieved from: https://www.ft.com/content/64539a44-6e87-11ea-89df-41bea055720b (accessed 30/11/2020).

Solon, O. (2017) 'China cracks down on VPNs, making it harder to circumvent Great Firewall', *Guardian* retrieved from: https://www.theguardian.com/technology/2017/jan/23/china-vpn-cleanup-great-firewall-censorship (accessed 30/11/2020).

Taddeo, M. (2013) 'Cyber Security and Individual Rights, Striking the Right Balance', *Philosophy & Technology* 26 (4), 353–356, https://doi.org/10.1007/s13347-013-0140-9.

UN General Assembly, (1966) 'International Covenant on Civil and Political Rights', *United Nations*. Treaty Series, 999, retrieved from: https://www.refworld.org/docid/3ae6b3aa0.html (accessed 30/11/2020).

UN General Assembly, (1999) 'Resolution 53/144: Declaration on Human Rights Defenders (A/RES/53/144)', *United Nations*, retrieved from: www.undocs.org/en/A/RES/53/144 (accessed 30/11/2020).

UN General Assembly, (2017) 'The safety of journalist and the issue of impunity', *United Nations*, retrieved from: https://documents-

dds-ny.un.org/doc/UNDOC/LTD/N17/380/92/PDF/N1738092.pdf?OpenElement (accessed 30/11/2020).

UN Human Rights Council, (2012) 'Resolution: The promotion, protection and enjoyment of human rights on the Internet.' *United Nations,* retrieved from: https://digitallibrary.un.org/record/731540?ln=en (accessed 30/11/2020).

UN Human Rights Council, (2016) 'The promotion, protection and enjoyment of human rights on the Internet (A/HRC/RES/32/13),' *United Nations,* retrieved from: https://www.refworld.org/docid/57e916464.html (accessed 30/11/2020).

UN Human Rights Council, (2020) 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', *United Nations,* retrieved from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement (accessed 30/11/2020).

United Nations, (no date) 'The Foundation of International Human Rights Law,' retrieved from: https://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html (accessed 30/11/2020).

United Nations, (1948) 'Universal Declaration of Human Rights', retrieved from: https://www.un.org/en/universal-declaration-human-rights/ (accessed 30/11/2020).

United Nations, (2019) 'UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools,' retrieved from: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736 (accessed 30/11/2020).

UN Special Rapporteur, (2017) 'Encryption and Anonymity follow-up report', retrieved from: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf (accessed 30/11/2020).

UN Special Rapporteur, (2019) "Report on the adverse effect of the surveillance industry on freedom of expression', *United Nations,* retrieved from: https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx (accessed 30/11/2020).

Wang, Y. (2020) 'In China, the "Great Firewall" Is Changing a Generation', *Human Rights Watch*, retrieved from: https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation (accessed 30/11/2020).

Yan, T. Y. (2019) 'China taking Big Brother to Central Asia', *Eurasianet*, retrieved from: https://eurasianet.org/china-taking-big-brother-to-central-asia (accessed 30/11/2020).

Yang, Y., Nian, L., Sue-Li, W., Qianer, L. (2020) 'China, coronavirus and surveillance: the messy reality of personal data', *Financial Times*, retrieved from: https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca (accessed 30/11/2020).