THE ROMANIAN JOURNAL OF SOCIETY AND POLITICS

Exploring the need for human-centred cybersecurity. The WannaCry Cyberattack

Claudiu Mihai CODREANU

Currently enrolled as a Ph.D. student at the Doctoral School of the National University of Political Science and Public Administration (SNSPA) Bucharest, Romania, Claudiu Mihai Codreanu focuses in his research on cybersecurity policies and strategies, e-democracy and digital authoritarianism. His most recent research paper, published by the Europolity journal, deals with the issue of state-sponsored cyberattacks during the first year of the COVID-19 pandemic.

e-mail: cl.codreanu@gmail.com

ABSTRACT

Cyber operations, especially cyberattacks, have emerged to become one of the most significant security threats for state actors in the last decade or so, but they have also become increasingly disruptive for individuals. Moreover, one path generally taken by governments, authoritarian and democratic alike, is trying to enhance cybersecurity at the expense of privacy and anonymity of individuals and groups, begging the question whether cybersecurity and cyberattacks can be studied from a less state-centric perspective, focusing on people. The literature on cybersecurity from the perspective of Critical Security Studies is still rather scarce, and there is a need of more research, a gap which I aim to fill through this paper. Critical International Relations theory emphasizes the societal factors and individuals, looking further than the state. Moreover, Critical Security Studies focus on the security of people, proposing a human-centred approach to security. For this research, I shall start by describing the role of the state in cybersecurity and how Critical Security Studies can relate to cybersecurity. Furthermore, I shall explore the possibility of designing a human-centred cybersecurity endeavour. There is a growing need for changing the focus to the individual, especially because of the nature of current cyberattacks and governments' responses. Following this, I shall focus the discussion on the relationship between Critical Security Studies and cybersecurity around the WannaCry global ransomware attack, which is regarded as one of the most disruptive cyberattacks in history.

Keywords:

■Critical Security Studies ■Cyberattacks ■Cybersecurity ■Human-centred cybersecurity ■WannaCry cyberattack.

Introduction

In the last 10 years, the importance and visibility of cybersecurity issues have increased considerably, as state actors begun using cyberattacks more frequently in a much more disruptive way than previously. The WannaCry ransomware cyberattack was one of the most disruptive global cyberattacks in history, and it managed to spread all over the world, affecting hundreds of thousands of computers (Greenberg: 2017; Christensen, Liebetrau: 2019). Even more, the ransomware spread on a large variety of computer systems and networks, affecting UK's National Health System and disrupting its activities, putting at risk the health and/or lives of patients. In addition to this, 2017 was the year of another transnational cyberattack, which actually started as a cyberattack targeting a single country. The NotPetya attack disrupted a large set of activities in Ukraine, but then it spread to other countries and it caused billions of dollars in damages (Perlroth, Shane: 2019). Both of the cyberattacks were based on a software vulnerability and exploit in Microsoft's Windows operating system, discovered by the US National Security Agency and stockpiled for further usage, until it was stolen by other state hackers, leaked online, and then used by other state-sponsored hackers (Greenberg: 2019; Newman: 2019). Thus, the NSA managed to indirectly decrease the level of security in the world, and especially in the cyberspace, whilst on a quest to increase the US national security, by employing the exploit against other states regarded as adversaries (Dunn Cavelty: 2014).

Since these two cyberattacks have been indirectly caused by a state-actor (the United States) who was attempting to improve and advance its security, adopting a pure state-centric view may not provide sufficient insights into the issue. Therefore, in this paper I shall use a human-centred approach to cybersecurity, in order to discuss both the cyberattacks and the issue of intelligence agencies stockpiling software vulnerabilities and exploits, taking into account the WannaCry ransomware campaign. The study starts by providing an overview of the relevant literature regarding Critical Security Studies (CSS), cybersecurity and the relationship between the two, as well as the literature on human-centred cybersecurity approaches. Furthermore, the study also focuses on the role of the state in cyberspace and cybersecurity, highlighting that intelligence agencies have a significant role and contribute to also maintaining states' role in cyberspace. Going further, the paper explores the concept of human-centred cybersecurity, focusing on the case of the WannaCry cyber campaign, which showcases the need of implementing an approach based on this concept, and also of discussing the state's role in cybersecurity. My argument is that cyberattacks such as WannaCry highlight the need of questioning state-centric views on cybersecurity and attempt to place humans at the centre of all endeavours regarding the processes of ensuring cybersecurity. Moreover, placing human beings at the centre of cybersecurity endeavours would bring more attention to the effects that malicious cyber activities and cybersecurity activities have on individuals, provided that ensuring security in cyberspace should not come at the cost of digital rights and freedoms. Even though the Critical Security Studies literature on cybersecurity is not very vast, it can significantly contribute to the research on cyberspace by considering the individual as the referent of security. In cyberspace this issue might be complicated, but it is important to discuss if and how CSS can relate to cyberspace and cybersecurity, and how its concepts can be used to create more knowledge. CSS stands for avoiding a state-centric approach or a statist point of view (Peoples, Vaughan-Williams: 2010), hence the role of the state in cyberspace needs to be further problematised, together with the potential role of individual human beings. Furthermore, in this study, human-centred cybersecurity, or a human-centred approach to cybersecurity, is viewed as an approach that puts human beings, and not states, at the centre of cybersecurity processes and endeavours. Human-centred cybersecurity is also referred to as human-centric cybersecurity in scholarly literature, but I shall use mainly the form of human-centred throughout the paper.

Key aspects of Critical Security Studies

Critical Security Studies (CSS), also sometimes referred to as the Welsh School, represents an International Relations (IR) school of thought based on a Marxian interpretation of the world and mainly on Critical Theory (or the Frankfurt School). CSS proposes an approach to the concept of security built from its broadening (expanding the scope of security beyond military issues), deepening (linking the way we perceive security to our understanding of the world) and extending (taking into account multiple actors and going beyond the state, mainly to individual human beings) (Peoples, Vaughan-Williams: 2010, pp. 17-18; Wyn Jones: 1999, p. 166).

The school of Critical Security Studies is built on a critique of statism and state-centric approaches, asserting that human beings are the fundamental referents of security. CSS argues that all threats, no matter the sector they are included in, affect people before anything else, and hence the state, represented in some abstract way, should not be the ultimate referent of security, but the very human beings, which constitute the state anyway, should be considered the primary referents of security (Peoples, Vaughan-Williams: 2010, pp. 23-32).

The Copenhagen school (represented mainly by Barry Buzan, Ole Wæver and Jaap de Wilde) contributed to a certain degree to Critical Security Studies, as it extended the concept of security by proposing five sectors of security: military, political, economic, societal and environmental. Moreover, it introduced the theory of securitization, which refers to the speech process through which an actor, mainly leading governmental figures, labels an issue as a security issue, thus justifying extraordinary measures. However, from a human-centred security perspective, securitization theory does not do enough by broadening the dimensions of security, as the state still holds a significant position (Nyman: 2013, pp. 51-60).

CSS does not use only state-centric approaches, extending the scope of security beyond military threats, and it “anchors the theory and practice of security in a broader concern with human emancipation” (Wyn Jones: 1999, p. 5). Thus, CSS assumes the goal or purpose of “emancipation”, which refers to freeing the people from constraints (human or physical) that refrain them from doing what they would choose to (Peoples, Vaughan-Williams: 2010, pp. 31-32). One of the main scholars of Critical Security Studies, Ken Booth, clarified the concept of emancipation in a 1999 paper, arguing that “‘Security’ means the absence of threats. Emancipation is the freeing of people (as individuals and groups) from those physical and human constraints which stop them from carrying out what they would freely choose to do” (Ken Booth: 2011p. 319).

A Critical Security Studies approach can be used in a state-centric research, but only if the research avoids being statist too (Yau: 2019, p. 37). Furthermore, CSS considers that "real security" can be built upon the concept of emancipation (ibid.). In some cases, the state does not act as the guarantor of security, but as a threat to its citizens (like in the case of authoritarian regimes), while sometimes only certain institutions of the state produce forms of insecurity for their own citizens. This supports the idea that significant threats can come even from their own state, even if it fundamentally attempts to provide a secure environment for its citizens (Krause, Williams: 1997, p. 44; Wyn Jones: 1999, p. 99). In other words, "both emancipatory and regressive actions can be pursued in the name of security" (Ken Booth: 2011, p. 289).

Untangling cyberspace and the role of the state

Cyberspace is both a physical and "socio-technological environment", consisting of the networked system of computers, servers and other digital devices that "interact in digital space" (Valeriano, Maness: 2015, p. 24). In other words, cyberspace comprises the hardware real-world elements used for accessing and interacting in the digital space, and also the elements created in the digital world. Furthermore, in the view of Thierry Balzacq and Myriam Dunn Cavelty, cybersecurity is "a multifaceted set of practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access" (2016, p. 183). In other words, cybersecurity can be understood as a set of practices and policies employed by a variety of actors to increase the security of cyberspace (Balzacq, Dunn Cavelty: 2016, p. 180).

Moreover, a cyberattack can be defined as:

> *"an electronic attack to a system, enterprise or individual that intends to disrupt, steal or corrupt assets where those assets might be digital (such as data or information or a user account), digital services (such as communications) or a physical asset with a cyber component"* (Hodges, Creese: 2015, p. 34).

Cyberattacks can have a major impact on society as a whole and on individuals too, as it became apparent after the Cambridge Analytica scandal, the Russian information operations targeting states' elections, and the Brexit referendum (Burton, Lain: 2020, pp.

6-7). A large part of cyber incidents are operations in which a state actor tries to steal classified or sensitive information from another state's institutions, meaning that a significant proportion of malicious cyber activity can be described as cyber espionage (Valeriano, Maness: 2015, p. 9). Cyberattacks have become increasingly common over the last decade or so, and are now used by individuals, state and non-state actors in various ways, and in pursuit of various interests and objectives. Additionally, since this research refers to the WannaCry ransomware campaign, the concept needs to be properly defined. The ransomware is a type of malware that tries to capitalize on people's fear of losing important data or being faced with permanent hardware damage. Ransomware lock or encrypt victims' computers and demand a payment, or a ransom, in exchange for unencrypting the data, which is not always the case (Kharraz et al.: 2015, p. 3).

The role of the state in cybersecurity and cyberspace has expanded since the first years of the Internet, with the state acquiring multiple roles throughout the years, as suggested by the research of Myriam Dunn Cavelty and Florian Egloff (2019). At the very beginning, from the 1980s and 1990s, the state had the sole role as the *owner of the networks*, followed by the new role of *problem owner* (or problem solver) in cybersecurity. Since the 2000s, the state acquired the role of the *originator of the problem*, as states started to become more active in cyberspace thus creating issues for other actors involved. The state still has the responsibility to protect its military and civil networks, thus being the *guarantor of its institutions' cybersecurity*. At the same time, the state plays the role of *partner* in relation with private companies, especially regarding critical infrastructures. Moreover, beside its role of a partner, the state also functions as *legislator and regulator* in relation with both private companies, institutions and citizens (Dunn Cavelty, Egloff: 2019, pp. 47-49).

However, cybersecurity increasingly depends on internet service providers (ISPs), private companies which operate critical infrastructure, and big tech companies overall, in particular Microsoft, Google, Facebook and Apple (Burton, Lain: 2020, p. 5). In many ways, cybersecurity is the "responsibility of every individual and every company" (Dunn Cavelty, Egloff: 2019, p. 48). Nevertheless, intelligence agencies, including military agencies, gained a significant role in cybersecurity and the cyberspace, both for offensive and defensive cyber operations, and it can be argued that they are the most important actors, especially in the strategic use of cyberspace (Burton, Lain: 2020, p. 2; Dunn Cavelty, Egloff: 2019, p. 47). The United States is regarded by scholars as the state most targeted by cyber espionage, and the second most active user of cyber espionage operations against other states, with the first being China (Valeriano, Maness: 2015, p. 9). According to Brandon Valeriano and Ryan Maness (2015), cyber espionage activities pursued by state-actors are the most common type of operations in cyberspace, and they can be broadly defined as an attempt by a government to steal important or confidential information from another government (p. 9). This suggests that the state has to work on finding the right balance between freedom and security in cyberspace, since giving more powers to security agencies can have a negative impact on civil rights in the digital space (Dunn Cavelty, Egloff: 2019, p. 51). Thus, as the CSS approach suggests, the process of enhancing security in cyberspace by expanding the mandate of responsible state's agencies comes against emancipation, and can actually produce insecurity for individuals, since the majority of the ways of enhancing security in cyberspace involve a negative trade-off of civil rights, such as anonymity and privacy.

Overall, in the race of enhancing offensive cyber capabilities, state actors actually manage to create more insecurities and endanger their own national security which they are trying to protect, and also indirectly endanger the national securities of other states, including allies. Intelligence agencies search for and exploit security flaws in various software and operating systems in order to gain the ability to access systems and networks for espionage, potential disruptive cyberattacks or surveillance. In some cases, intelligence agencies find or create the software vulnerabilities and use them later, as they can be exploited at any time as long as the victim does not detect the security flaw (Dunn Cavelty, Egloff: 2019, p. 47).

CSS's view on cyberspace and state practices in cybersecurity

Critical Security Studies literature on cybersecurity and cyberspace is rather scarce. Up until the 2010s, critical security literature focused almost entirely on the discursive process of cyber incidents, and devoted little attention to specific events or developments in cyberspace. However, in the last years, critical security literature moved further from analysing discursive constructions, and turned its focus to material aspects of cyberspace and cybersecurity, and on practice-related issues (Dunn Cavelty: 2019, pp. 139-140).

One downside of CSS's work on cybersecurity is that most of the literature does not take into account that "cyber-security is a type of security that enfolds in and through cyberspace, so that the making and practice of cyber-security is at all times constrained and enabled by this environment" (Balzacq, Dunn Cavelty: 2016, p. 179). Cybersecurity is produced by a multiplicity of actors, expanding across different sectors of society, from every individual computer user, CEOs, regulatory bodies and standardisation organisations, to computer security specialists and other. In this ecosystem, the role of politicians and government officials is secondary to those producing cybersecurity, since they can unravel various developments and events in cyberspace, take action in the form of statements (with the aim of securitization), and can create and implement policies (Balzacq, Dunn Cavelty: 2016, p. 180).

Challenges, risks and threats in cyberspace, and cybersecurity in general, go beyond state borders. The state is now far from being the single actor in cyberspace, even though it still has a central role. Private companies have become some of the most important players in the cyberspace and in cybersecurity too, especially because they own and operate the large majority of the ICT infrastructure. In addition to this, companies (like Microsoft or Google) develop software and digital devices used by state institutions, citizens, private companies and civil society in a big part of the world (Christensen, Liebetrau: 2019, pp. 395-397).

There are a lot of reasons for the critique of states' role in cyberspace, and also for avoiding a statist approach. Aiming to gain the ability to access more data and to prepare for potential conflicts, intelligence services over the world are actually making cyberspace more insecure in a direct way. For instance, it has been reported by the media and civil society since before 2013 that the NSA is actively engaging in acquiring and exploiting various zero-day vulnerabilities in software and hardware to inject its own malware in strategic locations in the Internet infrastructure. Thus, instead of alerting software vendors of vulnerabilities in order to patch them, intelligence agencies exploit them and keep them secret. Furthermore, it is unknown which software have vulnerabilities that can be exploited, nor which systems have been compromised. The backdoor programs injected in various software and hardware can be activated at any time and used for espionage, surveillance, and also for potential disruption. Thus, actors can employ actions with the aim of increasing security, which can also be responsible for making both cyberspace and the real word less secure, either directly or indirectly (Dunn Cavelty: 2014, pp. 702-710).

After the discovery of a software vulnerability, a security agency can alert the company developing the software in order to patch it, but the security flaw can also be used for offence, exploiting it stealthily and secretly. Because of this, thinking only in terms of cyber offence and cyberwarfare can play a significant part in creating cyberthreats and more cyber insecurity, in opposition to building a cybersecurity of and for the people, a healthy cyberspace. This can be done by consolidating people’s knowledge of cybersecurity and promoting an efficient cybersecurity culture (Yau: 2019, p. 47), proving the need for a human-centred approach to cybersecurity.

Nevertheless, exploiting such vulnerabilities means keeping security flaws unaddressed, and this reduces the security of the entire cyberspace, ultimately reducing security for everyone. Furthermore, it cannot be known if the backdoors are under the full control of the agency that created them, nor if anyone else discovered them, and hence these vulnerabilities can be exploited or identified by other state actors with potential malicious intents. Therefore, such actions taken by the state have become not only a threat for human security overall, but also for the very same state who employs the use of such vulnerabilities. Consequently, if states do not refrain from creating more vulnerabilities and security flaws in the system, then the race for enhancing national security will mean generating less cybersecurity, and hence less national security overall, taking into account the unpatched vulnerabilities left in critical infrastructures (Dunn Cavelty: 2014, pp. 710-711).

Even though some practices employed by the state constitute a major source of insecurity in cyberspace, a safe, secure and open cyberspace can only be created with the involvement of the state (Dunn Cavelty: 2014, p. 711). So, it is difficult to adopt a pure human-centred view regarding cyberspace. Nonetheless, this still means that a statist view can and sometimes should be avoided.

Practices that introduce vulnerabilities into the networks comprised in the cyberspace have a negative effect on the exercise of human rights of individuals everywhere and hence the usage of such practices should be heavily restricted and closely monitored. However, intelligence agencies may still retain the ability to request exceptions, as long as their actions and policies are as transparent as possible. For instance, the US government considers on a case-by-case basis whether it should disclose or keep secret the discovery of software vulnerabilities, both options aiming at increasing security. Nevertheless, from a human-centric standpoint, making cyberspace deliberately more insecure comes into opposition with the objective of securing cyberspace for all users. Consequently, these exceptions should be limited and publicly justified (Deibert: 2018, p. 415).

The main aspects of a human-centred cybersecurity approach

One significant reason for the disregard of human beings in cybersecurity research and/or policy making is the sole focus on digital equipment and technical systems as targets, also leading to responses taking into account only technology elements in cybersecurity. Computer systems, servers and other devices or equipment are non-human objects and they are indeed valuable for societies, but they cannot be considered entirely separated from human life. Cybersecurity is not only a technical concept in which networks or systems act as referents of security, and this can be seen even in states' cybersecurity strategies. Even though most of the threats included in this kind of strategies ultimately affect individuals, networks and computer systems are still perceived as the main object of security (Dunn Cavelty: 2014, pp. 706-707; Klein, Hossain: 2020, p. 6).

Cybersecurity should take into account the people's needs and not only those of the state. A human-centred cybersecurity approach focuses on digital privacy and the privacy of data, Internet freedom and the violations of digital human rights, aiming at employing policies and practices that empower individuals to freely exercise their rights. In addition to this, protecting critical infrastructures is crucial in this regard, as societies depend more and more on ICTs and individuals rely on their functioning in almost all aspects of life. Likewise, the same goes for providing a secure cyberspace for citizens (Liaropoulos: 2015, pp. 15-19; Klein, Hossain: 2020, p. 7).

Despite this, safeguarding and enhancing cybersecurity is an action that involves international organisations, private companies, individuals and non-governmental organisations across states, but also state actors. In the current environment, it can be argued that the state remains the main actor that can secure human needs. Moreover, the needs of humans are addressed in some ways by the state-centric or traditional view of security, since providing a safe and secure environment for a state's citizens is the main objective of the majority of national security policies. However, not all current policies regarding cybersecurity provide a secure cyberspace (Liaropoulos: 2015, pp. 18-19).

One of the milestones of developing a human-centred security approach, based on protecting the security and well-being of individuals and communities, was the 1994 Human Development Report of the UNDP (United Nations Development Program), which adopted the concept of human security. Furthermore, a human-centred cybersecurity approach is built upon the consideration that individuals and communities are both objects and subjects of cybersecurity, and it stands as a framework for developing and implementing policies placing human wellbeing and civil rights at the centre of cybersecurity policies (Zojer: 2020, pp. 358-360). Human security considers individuals and communities as the objects of security, and not the state, as opposed to traditional approaches to security. Thus, human security advances an approach based on linking well-being to a security centred on individuals (and communities) that safeguards the freedom from fear, want, vulnerability and indignity (Klein, Hossain: 2020, p. 6). More than this, human security issues, like the right to privacy or freedom of speech, should be seen as actually contributing to overall cybersecurity (in opposition with the current view), because increasing the proportion of encrypted data will help reduce both cybercrime and cyber espionage, which will benefit both state-centred and human-centred security (Dunn Cavelty: 2014, p. 711).

The human-centred approach to security positions human beings, no matter their citizenship, as the ultimate objects of security. Furthermore, a human-centric cybersecurity approach considers as primary objects of security the whole undifferentiated global network, and it aims to guarantee that the integrity of cyberspace is upheld worldwide. Yet, state actors are not ignored and they can still play a significant part as supporting institutions which have the objective of safeguarding the wellbeing and rights of individuals (Deibert: 2018, pp. 412-415).

An unprecedented global ransomware campaign, a Windows exploit and NSA's role

A ransomware campaign is a type of malware threating to publish data. After the malware infection, the ransomware tries to contact a server for the information it needs to activate, and afterwards all of the data on the PC is encrypted and held for ransom. Ransomware, like most malware, spread from infected Microsoft Word documents, PDFs or other files sent in emails, but it can also spread through computers that are already infected by malware which provide backdoors for access. After the files are locked, the infected computer shows only a message asking for a payment to decrypt the data, threating to destroy all of it if the payment is not made. Most of the time, ransomware include a timer so that victims are constrained to make the payment (Hern, Gibbs: 2017).

WannaCry is a perfect example of state institutions and state actors producing insecurity with the aim of enhancing security. The malware was based on a software vulnerability which the U.S. National Security Agency (NSA) stockpiled for cyber espionage and potential offensive cyber operations. The WannaCry ransomware spread in over 150 countries and affected hundreds of thousands of computer systems, causing widespread anxiety and fear, especially for individual users. Overall, the damages caused by the ransomware are estimated to have gone over 4 billion dollars. The ransomware attack became known on 12 May 2017, affecting over 300.000 computers around the world since. By some estimations, the group that stole and leaked the ransomware earned little over 50.000 dollars, so it can be argued that creating chaos, and not raising money, was their objective. For instance, the group behind the Angler ransomware campaign managed to gain over 60 million dollars before 2015 (Burton, Lain: 2020, p. 12; House of Commons: 2018, p. 4; Greenberg: 2017; BBC News: 2017).

Vulnerabilities discovered in common software can trigger access to a significant number of targets, and it can become a major asset for intelligence services. But, at the same time, the harm done by finding or creating a vulnerability in widely-used software can be greater than the advantage given by granting a backdoor. Stockpiling this kind of vulnerabilities and refusing to disclose them to the affected companies or to the public represents a risk for the citizens of which the security agency tries to protect, but also to citizens of other countries. Failing to disclose a zero-day software vulnerability can lead to its discovery by other governments or malicious cyber actors who can exploit the vulnerability against other states or even against the state which discovered it, causing potential widespread disruption, as in the case of WannaCry. Thus, governments attempt to balance between keeping the vulnerability secret for future usage and also safeguarding their own citizens, companies or institutions from the vulnerability (Christensen, Liebetrau: 2019, p. 402).

The vulnerability of the ransomware, the so-called kill switch, was actually discovered by a malware analysis expert. Thus, the cyberattack was stopped by an individual and not by national security agencies (Burton, Lain 2020, p. 13). The kill switch was actually built inside the malware's code, and the malware expert who stopped the attack just had to register the domain which the malware tried to contact for encrypting the files (Greenberg: 2017).

The group of hackers who launched the WannaCry global ransomware campaign acquired the EternalBlue exploit discovered by the NSA sometime before 2016. However, cybersecurity company Symantec discovered that the EternalBlue exploit was obtained by a Chinese hacking group back in 2016, and it was already used in an espionage campaign, but it ultimately was the Shadow Brokers group who made in public. In 2016, the Russian group Shadow Brokers posted five leaks of hacking tools which were stolen from the National Security Agency, most probably with the aim of discrediting the NSA and the US. The exploit was named EternalBlue by the NSA, and it was included in the hacking group's final leak. However, the NSA did in fact announce Microsoft about the vulnerability after it was stolen and before it was leaked online, and hence the security flaw was patched by the company in a software update one month before Shadow Brokers released the hacking tool (Hern: 2017; Greenberg: 2019).

The WannaCry ransomware campaign hit UK's National Health System (NHS), Spain's Telefonica company, it affected German railroads and over 200.000 organizations around the world. The cyberattack infected a significant part of NHS's computers in just six hours, as the malware spread from computer to computer through networks (Hern, Gibbs: 2017; Perlroth, Shane: 2019). Because of the ransomware, NHS hospitals had to cancel around 20.000 appointments and operations, and some patients in the affected hospitals' emergency departments even had to be diverted or transferred to other hospitals (House of Commons: 2018, p. 4).

US and UK accused North Korea for the WannaCry ransomware attack and publicly declared Pyongyang was responsible (BBC News 2017). Nonetheless, the ransomware was based on a vulnerability extracted from publicly leaked NSA documents and tools which encrypts the content of Windows PCs, demanding an online payment for decrypting the data (Hern, Gibbs 2017). The White House and the NSA denied any responsibility for not disclosing the vulnerability (Christensen, Liebetrau: 2019, p. 401).

As stated by a 2018 UK House of Commons report on the cyberattack, hospitals could have prevented the spread and effect of the ransomware by updating the operating systems (OS) and installing Microsoft's patch for Windows 7. Moreover, hospitals were alerted by the NHS to install the security patch, but there was one significant issue – applying patches and updates to medical equipment's operating systems can disrupt its operation and can constitute a clinical risk to patients (House of Commons: 2018, p. 12).

Despite being the first ransomware campaign, WannaCry is not the only cyberattack based on the EternalBlue exploit stolen from the NSA. In June 2017, Russian military intelligence combined EternalBlue with another tool leaked from the NSA (EternalRomance) and targeted Ukraine. The NotPetya cyberattack, which was designed to look like a common ransomware, but aiming at destroying the data, wiped about 10% of Ukrainian computers. Moreover, the attack spilled over beyond Ukraine's borders, causing major disruptions in companies as Maersk, FedEx and Merck, the damage done being estimated at more than 10 billion dollars. Nevertheless, the use of the exploit made full circle around the globe and the US was also targeted by Russia, Russian hackers using EternalBlue to compromise hotel Wi-Fi networks (Greenberg: 2019; Perlroth, Shane: 2019).

In 2019, EternalBlue was allegedly used by hackers in a ransomware campaign against Baltimore local authorities in the US, freezing thousands of computer systems and disrupting digital services like platforms used for paying for utilities and taxes, but also for sending health alerts and so on. The cyberattack also disrupted other activities of the city authorities, as the staff was unable to use email services from their accounts. The authorities decided to not pay the ransom, which consisted in 13 Bitcoin (accounting then for over 100.000$), but the computers remained locked and the services frozen (Perlroth, Shane: 2019; BBC News: 2019).

The NSA did not accept its responsibility for choosing not to disclose the discovered vulnerability and for creating, failing to secure and losing control of the exploits. The US agency has never officially made a comment on the issue and it never disclosed exactly what led to losing control of the hacking tools (BBC News: 2019). However, since 2010 the US has implemented the Vulnerabilities Equities Process program, which requires the disclosure of zero-day vulnerabilities and exploits by intelligence agencies to other government agencies, in order to review them and decide if they can be kept secret or if they need to be disclosed to affected companies (Newman: 2017).

Towards a human-centred cybersecurity approach. Is it possible to overcome existing challenges?

The cyberspace, as well as cybersecurity ideas and policies have evolved considerably in the last 10-15 years. Nowadays, the majority of the world's states have adopted national cybersecurity strategies or they at least incorporated cybersecurity issues into their national security strategies. Moreover, even though the role of private companies increased over time, states still play a major role in cyberspace, both in practice and policy making, especially when it comes to intelligence services (Dunn Cavelty, Egloff: 2019; Balzacq, Dunn Cavelty: 2016; Dunn Cavelty: 2014). Private companies, besides owning large parts of the infrastructure, have become key cybersecurity providers, even for states.

Thus, the question remains: where do individual human beings fit into this whole development? It seems that individuals and communities were rather left behind all of this progress, even though they are the main beneficiaries of the progress in technology and the Internet of Things, and, more importantly, among the main targets of malicious cyber activity, both in form of cyberattacks and cybercrime. In matters of individuals' and communities' role in cyberspace and cybersecurity, it can be argued that they are still considered to be only weak links in ensuring a sound national cybersecurity, and also that their digital freedoms are obstacles for enhancing national cybersecurity. In these matters, progress is yet to be made. For example, the 2020 European Union Cybersecurity Strategy highlights the need to protect human rights and freedoms in the cyberspace, aiming to ensure that digital technologies are human-centric and that the Internet remains open, free and global (European Commission: 2020, pp. 19-20).

Taking into account the main considerations and proposals of Critical Security Studies, such as the broadening, deepening and extending of security, avoiding state-centric approaches, identifying human beings as the ultimate referents of security and considering emancipation as an objective, developing a human-centred cybersecurity is a rather difficult endeavour. In the particular case of the WannaCry ransomware attack, the argument for the need of a human-centred cybersecurity can be made more easily. Hospitals and medical equipment were affected, computer systems and networks were disrupted, but human beings, individuals, were ultimately the most impacted, since critical health services were disrupted (Hern: 2017; House of Commons: 2018). While there were no reports of patients severely affected by the disruption, and thankfully no direct or indirect fatalities, few efforts have been made to mitigate the direct impact it had on the people (House of Commons: 2018; Christensen, Liebetrau: 2019). Thinking exclusively in military terms, or from a state-centric perspective, leaves out a multiplicity of issues, actors, developments and potential actions to improve cybersecurity. Issues regarding cyberspace go beyond the state, both inwards and outwards, from state institutions to private companies, NGOs, communities, individuals, as well as outside state borders, to other states and international or transnational organisations and networks.

Nevertheless, is a human-centred approach possible in cybersecurity? We argue that an approach focusing on individuals and communities is possible, but the state cannot be completely left out of the problem. While the state can be a creator of insecurity, it can still contribute to increasing cybersecurity and there are few ways of going around it to majorly improve cybersecurity overall. This may not be the case with authoritarian regimes, but in the case of liberal democracies, even if some security agencies actively decrease security directly or indirectly, there can be some workarounds.

Since the state is both security guarantor and insecurity creator, can it refrain from using vulnerabilities if other states act in the same matter? The answer may very well be yes. Less vulnerabilities in software also means less potential security breaches inside the state, and less opportunities for malicious cyber campaigns (Dunn Cavelty: 2014). In addition to this, even if other state or non-state actors are discovering exploitable vulnerabilities, if one state’s intelligence agency would work on identifying security flaws and rapidly alert software vendors, the vulnerabilities would get patched faster resulting in less damage overall (Christensen, Liebetrau: 2019; Dunn Cavelty: 2014). Of course, this leaves out the strategic opportunity of exploiting the vulnerability in favour of said intelligence agency, which would contribute to enhancing cybersecurity overall. Even so, intelligence agencies can make the argument that some security flaws need to be stockpiled and exploited as they are essential for cyber defence activities, gaining the ability to know beforehand of an adversary actor’s plans or actions. That would also mean that the security agencies must be held responsible if they lose control of hacking tools and exploits, and if they indirectly or directly cause disruption or put at risk their citizens.

As smart technologies are becoming more widespread, one should ask which argument would be used in the future for hiding a security flaw in the software or hardware of a smart electric vehicle, even a self-driving bus. By exploiting the vulnerability, the state would be able to use it for surveillance, disruption, or for other purposes, but failing to inform the software vendor would also mean that other malicious actors, state or non-state, have the possibility of exploiting the vulnerability for more disruptive purposes (Newman: 2017; Dunn Cavelty: 2014; Christensen, Liebetrau: 2019). Likewise, preinstalling backdoors on digital devices would make intelligence agencies’ work easier, but that would also mean that individuals become more vulnerable to hackers, too. This is also why having the ability to use encrypted messaging services matters in cyberspace, from a human-centred point of view. If the services already have a flaw in its design, it can be exploited by cyber criminals too.

Therefore, a human-centred approach cybersecurity approach is to a certain degree possible. In other words, there is a great need to pay more attention to individuals and communities regarding cybersecurity, but it is rather difficult in the current context to place them in a central point regarding all issues, or in the focus of the whole cybersecurity endeavour. What needs to be done is granting individuals a greater role in cybersecurity policymaking and practices, and taking them into account when those policies are being developed and implemented. Cybersecurity policies and practices should also consider the online experience of minority or marginalised groups, based on gender or gender identity, romantic orientation and on ethnic or religious background, as these groups are more vulnerable to malicious cyber activities than the average population (Burton, Lain: 2020, p. 16). Moreover, attention should also be focused on civil society groups and activists, political groups, journalists and so on, as these groups are also more likely to become targets of various cyber operations.

In addition to this, actors in cyberspace should rely more on resilience-based policies and practices, such as promoting a culture of cybersecurity and implementing activities to ensure networks' security, internal security and device security, computer hygiene habits, which can be done by both designated cybersecurity experts and individual users alike (Valeriano, Maness: 2015, p. 207). These activities should not be limited to governments, since civil society groups and other organisations should play a greater role in promoting a culture of cybersecurity among the general population, institutions, academia and journalists alike. Furthermore, when it comes to scientific endeavours, cyberspace and cybersecurity can and should be studied from a Critical Security Studies perspective and from a human-centred point of view, as this perspective can fill many gaps in the efforts of finding ways of safeguarding cyberspace. The most important proposal brought forward by CSS is that security in cyberspace cannot be increased at the expense of the rights and freedoms of individuals. Doing so would only mean decreasing security for individuals, which ultimately means decreasing national security overall. Cybersecurity should be ensured as a collective effort of all actors involved in the process, and also of all actors, individuals, groups or organisations affected by malicious cyber operations and by cybersecurity policies that can restrict digital rights or those that can contribute to a more vulnerable cyberspace.

Conclusion

Linking Critical Security Studies and cyberspace is not a straight-forward endeavour, but it is an attempt that must be worked upon. Critical Security Studies are not problem-solving theories, so research does not necessarily produce proposals or suggestions for state institutions or other types of government. Nonetheless, CSS can be used for analysing and problematizing cybersecurity and issues regarding cyberspace, which is a complementary perspective, since most research is focused on specific problems, issues, developments or incidents, and there must be times when a researcher must question if problems arise because of how the whole environment is constructed. This may not always be the case, but for cyberspace, avoiding a statist view in research may be helpful in order to produce more knowledge and gain a further understanding of the whole context. In addition to this, using a human-centred cybersecurity approach is helpful considering that, in many cases, the state decreases the level of security in cyberspace in the effort of protecting its own security.

Both progress and issues in cyberspace develop rapidly, and so cybersecurity is a very dynamic issue to study and more research is needed. Latest cyberattacks against the US, the surge of cybercrime and state-sponsored cyber operations during the COVID-19 pandemic are only a part of the type of developments and problems that can arise from vulnerabilities in cyberspace, and so they need to be properly addressed and studied to prevent future serious damage across societies.

References

- Balzacq, T., Dunn Cavelty, M (2016), "A theory of actor-network for cyber-security", *European Journal of International Security*, 1(2): pp. 176-198.

- BBC News (2017), „Cyber-attack: US and UK blame North Korea for WannaCry", *BBC*, December 19, accessed November 10, 2021, https://www.bbc.com/news/world-us-canada-42407488.
- BBC News (2019), "Baltimore ransomware attack: NSA faces questions", BBC, May 27, accessed November 10, 2021, https://www.bbc.com/news/technology-48423954.
- Booth, K (1991), "Security and emancipation", Review of International Studies, 17(4), pp. 313-326.
- Booth, K (2011), "Critical Security Studies", in D. J. Christie (ed.), *The Encyclopedia of Peace Psychology*, Blackwell Publishing, Chichester.
- Burton, J., Lain, C (2020), "Desecuritising cybersecurity: towards a societal approach", *Journal of Cyber Policy,* 5(3), pp. 449-470.
- Christensen, K. K., Liebetrau, T (2019), "A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry", *Intelligence and National Security* 34(3), pp. 395-408.
- Deibert, R. J (2018), "Toward a human-centric approach to cybersecurity", *Ethics & International Affairs*, 32(4), pp. 411-424.
- Dunn Cavelty, M., Egloff F. J (2019), "The politics of cybersecurity: Balancing different roles of the state", *St. Antony's International Review* 15(1), pp. 37-57.
- Dunn Cavelty, M (2014), "Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities", *Science and engineering ethics* 20(3), pp. 701-715.
- Dunn Cavelty, M (2019), "The materiality of cyberthreats: securitization logics in popular visual culture", *Critical Studies on Security* 7(2), pp. 138-151.
- European Commission (2020), *The EU's Cybersecurity Strategy for the Digital Decade*, Brussels, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.
- Greenberg, A (2017), "The Wannacry Ransomware Hackers Made Some Real Amateur Mistakes", *Wired*, May 15, accessed November 10, 2021, https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes.
- Greenberg, A (2019), "The Strange Journey of an NSA Zero-Day—Into Multiple Enemies' Hands", *Wired*, May 7, accessed November 10, 2021. https://www.wired.com/story/nsa-zero-day-symantec-buckeye-china/.
- Hern, A, Gibbs, S (2017), "What is WannaCry ransomware and why is it attacking global computers?", *The Guardian*, May 12, accessed March 16, 2021, https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20.
- Hern, A (2017), "Who is to blame for exposing the NHS to cyber-attacks?", *The Guardian*, May 15, accessed November 10, 2021, https://www.theguardian.com/technology/2017/may/15/who-is-to-blame-for-exposing-the-nhs-to-cyber-attacks.
- Hodges, D., Creese, S (2015), "Understanding cyber-attacks", in J. A. Green (ed.), *Cyber Warfare: A multidisciplinary analysis,* Routledge, New York.

- House of Commons (2018), *Cyber-attack on the NHS*, accessed November 10, 2021, https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf.
- Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E (2015), "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks", in M. Almgren, V. Gulisano and F. Maggi (eds.), *Detections of Intrusions and Malware, and Vulnerability Assessment, 12th International Conference, DIMVA 2015 Milan, Italy, July 9-10, 2015, Proceedings*, Springer, Cham.
- Klein, J., Hossain, K (2020), "Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change", *Arctic Review* 11, pp. 1-18.
- Krause, K, Williams, M. C (1997), "From Strategy to Security: Foundations of Critical Security Studies", in K. Krause and M. C. Williams (eds.), *Critical Security Studies: Concepts and Cases*, UCL Press, London.
- Liaropoulos, A (2015), "A human-centric approach to cybersecurity: Securing the human in the era of cyberphobia", *Journal of Information Warfare* 14(4), pp. 15-24.
- Newman, L. H (2017), "Why Governments Won't Let Go of Secret Software Bugs", *Wired*, May 16, accessed November 10, 2021. https://www.wired.com/2017/05/governments-wont-let-go-secret-software-bugs/.
- Nyman, J (2013), "Securitization theory", in L. J. Shepherd (ed.), *Critical Approaches to Security: An introduction to theories and methods*, Routledge, New York.
- Peoples, C., Vaughan-Williams, N (2010), *Critical Security Studies: An introduction*, Routledge, New York.
- Perlroth, N., and Shane, S (2019), "In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc", *The New York Times*, May 25, accessed November 10, 2021, https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html.
- Valeriano, B., Maness R. C (2015), *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford University Press, New York.
- Wyn Jones, R (1999), *Security, Strategy, and Critical Theory*, Lynne Rienner Publishers, Boulder.
- Yau, H (2019), "A critical strategy for Taiwan's cybersecurity: a perspective from critical security studies", *Journal of Cyber Policy* 4(1), pp. 35-55.
- Zojer, G (2020), "Moving the Human Being into the Focus of Cybersecurity", in M. Salminen, G. Zojer, K. Hossain (eds.), *Digitalisation and Human Security: A Multi-Disciplinary Approach to Cybersecurity in the European High North*, Palgrave Macmillan, Cham.