

CYBER-SECURITY AS AN ISSUE OF THE CONTEMPORARY SECURITY AGENDA

Basri Kastrati

Deputy Ombudsman, Kosovo

Basri.Kastrati@oik-rks.org

Aleksandar Pavleski

Faculty of Philosophy - Skopje, Institute for Security, Defence and Peace

pavleski@fzf.ukim.edu.mk

Nikolčo Spasov

Faculty of Detectives and Security

nikolco.spasov@fon.edu.mk

Abstract

Today's complicated security environment increasingly initiates new security risks and threats globally, which on the one hand, very easily cross the national borders of states, and on the other hand, also easily overcome traditional security capacities and responses of the states aimed at achieving and strengthening their security. In this context, we are witnessing that states, including state and private entities within national frameworks, are increasingly exposed to the so-called cyber threats, which, if not effectively prevented, seriously threaten the normal functioning of the state. Moreover, we face a constantly evolving and expanding landscape of threats, and increasingly sophisticated attacks that blur the lines between cyberattacks and cyber espionage. As a result, cyber security is increasingly emerging as a new, serious issue in the contemporary security agenda as well as in security studies, which are faced with the challenge of its proper conception within national, regional and international security approaches and practices. In this context, the paper analyzes the so far attempts, as well as the opportunities and challenges in offering a clear definition and a clear conceptualization of cyber security as a significant object and matter of the contemporary security agenda.

Keywords: *security agenda, cyber-security, cyber-threats, critical infrastructure*

1. INTRODUCTION

The use of internet is rapidly expanding and has become the core component of everyday society. Still, the digital transformation of the societies has inevitably opened the space to new, so-called cybersecurity threats. Actually, easy access to data brings along severe security issues. It is no doubt that despite its many benefits, cyberspace has, at the same time, opened doors for those intent on achieving criminal goals. Among other aspects, it is strongly confirmed, by cyber blackmail, identity theft and fraud, attacks on various branches of the critical infrastructure of states, including the energetic grids, communication networks, and financial and transportation systems. Moreover, during the Covid-19 pandemic, public institutions as well as private companies had to adapt to remote working and this created more possibilities for cybercriminals. The war in Ukraine has also affected

cybersecurity. As a result, protection against cyber threats has become essential for properly society function. Cyberattacks can prove very costly. According to the European Commission, the annual cost of cybercrime to the global economy is estimated to have reached €5.5 trillion by the end of 2020 (EC, 2023).

In this regard, contrary to the previous, dominant understanding of cyber security mainly through the prism of technological debates, dilemma about the placement of cyber security in the context of the security agendas is being increasingly raised. A cyber threat has the potential to breach all levels of security very quickly due to the speed with which actions can occur and the extent of its interconnectedness. In addition, the use of the term cyber conflict is increasingly being promoted in security debates. Valeriano and Maness have defined cyber conflict as: “the use of computational technologies in cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities” (Valeriano & Maness, 2015). As a result, implementing effective measures to secure cyberspace remains a difficult and challenging issue. Actually, there is a growing understanding that such insecurities are driving countries to channel the ever-increasing resources into their ability to defend themselves against cyber actions, and to launch offensive operations. On the other hand, such situation can be connected with the so-called security dilemma approach and in that context to initiate a new one, the so-called cyber arms race. Namely, in its traditional conceptualization, the arms race stems from mutual insecurity and the need to defend against an external threat. It follows that the insecurity in the cyber space also initiates the need of the states to defend against cyber threats, which in turn enables the positioning of cyber security within the contemporary security agenda. Actually, it is no doubt that the development of cyberspace has put states in an “unprecedented situation”, characterized by high levels of uncertainty as they try to maintain control in the face of a changing global security environment.

Therefore, from the contemporary security agenda perspective, countries should play a central role in addressing cyber threats to national security because they remain the actors with the power and authority to improve defenses against most existential cyber threats. In this regard, paper analyzes cyber security and cyber threats as part of the wider security agenda as well as a part of the necessity for contemporary approaches of the states in reducing their vulnerability and consequently increasing their cyber resilience.

2. CYBER SECURITY UNDERSTANDING

Cyber is a prefix derived from the word cybernetics and has acquired the general meaning through the use of computer. It is also used synonymously with cyberspace. Cyberspace connotes the fusion of all communication networks, databases and sources of information into a vast, tangled and diverse blanket of electronic interchange. Thus, a “network ecosystem” is created, a place that is not part of the normal, physical world. It is virtual and immaterial, a bioelectronics environment that is literally universal (Cavelty, 2010). It exists everywhere where there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves (Dyson et al., 1994)

Cyberspace is defined by Nye as the: “Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications” (Nye, 2010). Cyberspace refers to not only “all of the computer networks in the world”, but also to “everything they connect and control” (Clarke & Knake, 2010), highlighting the potential risk to a nation’s infrastructure given the fact that these systems are often dependent on internet networks.

Bearing in mind the above mentioned, it follows that cyber-security is concerned with making this bioelectronics environment safe. Actually, it refers to a set of activities and measures, technical and non-technical, intended to protect the real geography of cyberspace but also devices, software, and the information of data they contain and communicate, from all possible threats.

According to Škanata, cyber security is commonly defined as the practice of protecting computers, networks, programs and data from unauthorized access or malicious attacks that are aimed for exploitation. Hence, cyber security is focused primary on malicious activities prevention and protection from occurring (Škanata, 2020).

As a result of the broad context of the term cyber space, the term cyber security also incorporates more, so-called types of security. As such it can be noted:

- *Network security*, is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware;
- *Application security*, focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed;
- *Information security*, protects the integrity and privacy of data, both in storage and in transit;
- *Operational security*, includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella;
- *Disaster recovery and business continuity*, define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources;
- *End-user education*, addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

It follows that cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. Actually, such indicated types of security in cyberspace, confirm that cyber security must be analyzed and understood through the prism of a broader and more complex approach. It is much more needed especially in term of creating and developing of effective strategy for preventing and dealing with threats in this space.

3. CYBER THREATS AND INSECURE ENVIRONMENT

In general, threats that could potentially damage cyberspace are categorized as: failures, accidents and attacks, in information security, even though these categories are not necessarily mutually exclusive or always easily distinguishable.

The first ones, the failures, are mainly caused by deficiencies in the system or in an external element on which the system depends. As such, they may be connected to the software design errors, hardware degradation, human error or corrupted data. The next ones, accidents, include the entire range of randomly occurring and potentially damaging events. Actually, they are usually externally generated events (i.e., originate from outside the system), whereas failures are internally generated events. The last ones or the attacks, are mainly orchestrated by an adversary, and are generally referred to as hacker attacks (Cavelty, 2010). Hence, it should be noted that “hacker” is a loose term and has various meanings. Generally, the term “hacker” refers to someone who breaks into computer networks for the happiness he gets from the challenge of doing it or with some other intentions like stealing data for money or with political motivations (Spasova & Spasov, 2017). As a result, hackers are classified to different types, but mainly in terms of so-called White Hat and Black Hat hackers.

A White Hat hacker is a computer network security professional and has a non-malicious intent whenever he breaks into security systems. A White Hat hacker has a deep knowledge in Computer Networking, Network Protocols and System Administration, at least three or four Operating Systems and very good skills in Scripting and Programming. A White Hat hacker has the skills to break into networks but he uses his skills to protect organizations. A White Hat hacker can conduct vulnerability assessments and penetration tests are also known as an Ethical Hacker. Often White Hat hackers are employed by companies and organizations to check the vulnerabilities of their network and make sure that no hole is available in their network for an intruder. (Bala Chowdappa et al, 2014). On the other side, a so-called Black Hat hacker, as well known as a cracker, is a computer professional with deep knowledge in Computer Networking, Network Protocols and System Administration (at least three or four Operating Systems and very good skills in Scripting and Programming). He has also a good knowledge in many hacking tools and know how to program hacking tools, but contrary to the previous one, he uses his skills for unethical reasons. Actually, such hacker almost always has malicious intention for intruding a network (e.g., stealing research data from a company, or stealing money from credit cards, hacking email accounts, etc. (Bala Chowdappa et al, 2016).

Beside the mentioned White and Black Hat hackers, there is also and so-called Grey Hat hacker, who does the hacking without the permissions from the administrators of the network he is hacking. Still, he will expose the network vulnerabilities to the network admins and offer a fix of the vulnerability for money. A Script Kiddie is basically a hacker amateur who does not have much knowledge to program tools to break into computer networks. He often uses downloaded hacking tools from the internet written by other hackers or security experts (David, 2004). A Hacktivist is a hacker with political intentions. The hacktivist has the same skills as that of a hacker and uses the same tools as the hacker. The primary intention of a hacktivist is to bring public attention to a political matter. Phreaker is a telecom network hacker who hacks a telephone system illegally to make calls without paying for them.

According to the Threat Landscape 2022 report by the European Union Agency for Cybersecurity, there are eight prime threat groups:

- Ransomware hackers seize control of someone’s data and demand a ransom to restore access. Data quoted by the EU Agency for Cybersecurity shows that the highest ransomware demand grew from €13 million in 2019 to €62 million in 2021 and the average ransom paid doubled from €71,000 in 2019 to €150,000 in 2020. It

is estimated that in 2021 global ransomware reached €18 billion worth of damages – 57 times more than in 2015.

- Malware software that harms a system - includes viruses, worms, Trojan horses and spyware. After a global decrease in malware linked to the Covid-19 pandemic in 2020 and early 2021, its use increased heavily by the end of 2021, as people started returning to the office. The rise of malware is also attributed to crypto-jacking (the secret use of a victim's computer to create cryptocurrency illegally) and Internet-of-Things malware (malware targeting devices connected to the internet such as routers or cameras).
- Social engineering threats: exploiting human error to gain access to information or services - tricking victims into opening malicious documents, files or emails, visiting websites and thus granting unauthorized access to systems or services. The most common attack of this sort is phishing (through email) or smishing (through text messages).
- Threats against data: targeting sources of data to get unauthorized access and disclosure - Threats against data can be mainly classified as data breaches (intentional attacks by a cybercriminal) and data leaks (unintentional releases of data). Money remains the most common motivation of such attacks.
- Threats against availability - Denial of Service: attacks preventing users from accessing data or services. These are some of the most critical threats to IT systems. They are increasing in scope and complexity. One common form of attack is to overload the network infrastructure and make a system unavailable.
- Threats against availability: threats to the availability of the internet. These include physical take-over and destruction of internet infrastructure, as seen in occupied Ukrainian territories since the invasion, as well as the active censoring of news or social media websites.
- Disinformation/misinformation: the spread of misleading information. The increasing use of social media platforms and online media has led to a rise in campaigns spreading disinformation (purposefully falsified information) and misinformation (sharing wrong data). The aim is to cause fear and uncertainty.
- Supply-chain attacks: targeting the relationship between organizations and suppliers. This is a combination of two attacks - on the supplier and on the customer. Organizations are becoming more vulnerable to such attacks, because of increasingly complex systems and a multitude of suppliers, which are harder to oversee (European Union Agency for Cybersecurity, 2022¹).

As a result of all above mentioned, it follows that several characteristics or group of threats help to establish the perception of cyberspace as an inherently insecure environment. Still, from the paper analysis perspective, it should be noted that so-called “cyber weapons” are essentially “computer codes” used to inflict harm (Rid & McBurney, 2012), meaning that unlike the physical warfare domain, the virtual nature of malware makes it very difficult for states to gain an accurate picture of one another's capabilities. The anonymity that cyber methods can provide the attacker and the resulting attribution problem add to this uncertainty. Cyber capabilities include the malicious code created and the units mobilized, and the hardware and software developed, to defend against such code. Since cyber technologies can be much cheaper than conventional weapons, weaker states can possibly gain asymmetric advantages by entering into the cyber arms arena and compete on a more

even footing with traditionally powerful states. The sources of threat are therefore potentially more widespread.

4. CYBER SECURITY AS AN ISSUE OF THE CONTEMPORARY SECURITY AGENDA

As mentioned above, risks and threats in cyberspace are not sufficient to be part of the technological debates alone, but because of the entities that can carry them out (e.g., terrorists, criminals, etc.), as well as the entities that they target and their vulnerability, the need to analyze cyber security and from the national security aspect of the states is clearly highlighted. Actually, taking into account the consequences so far, and those that states may face as a result of various kinds of cyberattacks, the need to locate cyber security in the wider field of the contemporary security agenda inevitably arises.

In theoretical point of view, probably the most acceptable framework for analyzing cyber security as part of the security agenda is offered by the securitization theory of the Copenhagen School of Security Studies. Namely, in contrast to the previous, neo-realist understanding of security mainly through the prism of the military dimension, the theory of securitization opens up the possibility of a broader and deeper analysis of risks and threats in the security sphere. In addition, the referent object being threatened can encompass any actor from the individual to international level, including such actors as corporations, nations, states, and communities (Buzan et al, 1997). In this sense, cyber threats would clearly constitute security issues for a referent object even if the actor is an individual and the existential threat is a threat of economic ruin. In addition, a cyber-threat has the potential to span all levels of security very quickly based on the speed with which actions can occur as well as based upon inter-connectedness between many actors in this sphere.

In this regard, there are examples of cyber-attacks on the critical infrastructure in several countries in the past 10-year period, that have equally initiated consequences on both states and people as reference security objects. The first publicly acknowledged successful cyberattack in this sense is related to the hacking of power grid in two western regions of Ukraine, which resulted in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours in December 2015. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors (CISA, 2021) The attack set an ominous precedent for the security of power grids around the world. However, the electricity distribution system in Ukraine was again targeted in 2016.

In 2019, Germany suffered the largest hacker attack in the history. Hundreds of politicians from the Bundestag were targeted, including Chancellor Angela Merkel and President Steinmeier (KonBriefing, 2020). Sensitive information about politicians such as mobile phone numbers, contact information, credit card details, banking and financial details as well as private conversations were leaked through an anonymous Twitter account.

The next 2020, Germany was again the target of a cyber-attack in which, through an attack on the software of a hospital in Dusseldorf, it was impossible to treat emergency patients. According to KonBriefing's report for the first half of 2022, there were 42 cyberattacks in Germany, across a variety of industries, ranging from education and healthcare to finance, food, etc. (KonBriefing, 2022).

Such examples show that the potential for existential threats to the security of states and individuals can exist via cyberspace. In fact, cyber-attacks, especially those targeting critical infrastructure, initiate an equally worrisome level of vulnerability for both national and individual security values. Therefore, cyber security can be and should be viewed from

the standpoint of national and human security as well. As a result, it follows that models used to understand national security should also be applicable to studying cyber security issues.

Actually, it can be argued that cyber-security and national security do not differ in their core- both connote a condition that is free of (real or imagined) danger. The word security in general use is synonymous to being safe but especially as a technical term security means not only that something is secure, but also that it has been secured. It refers to the degree of protection resulting from the application of needed activities and measures (Fisher, 2005). The notion of security thus includes the practice of making something secure by securing it. It is therefore both a state of being and an activity of practice. It can further be argued that cyber-security and national security are even concerned with the same threat subjects ranging from terrorists to enemy states (though this has something to do with threat clustering) (Cavelty, 2010). Regarding the issue of clustering threats in cyber security, there is no doubt that technical development has a decisive role in the way threats are presented and perceived. Therefore, at the beginning there was a particular focus on cyber-crime and attacks on business networks. This was discursively interlinked with classified information and the foreign intelligence threat and thus elevated to a national security level.

Given such connection of cyber security to national and individual security, there is no doubt that it should be part of the contemporary security agenda. Still, in this regard the dilemma surrounding about the necessary actors involved in both national and cyber-security should be highlighted. Actually, computer experts are also professionals of security. And while the security of information systems is, in its pure form, concerned with technical measures to ensure that information flows as it should, national security measures include much more, such as the maintenance of armed forces, the maintenance of intelligence services to detect threats and civil defence measures. However, with the advent of cyber-security on the security policy agenda, the two notions begin to merge in strange ways. National security today is also concerned with attempts to create resilience and redundancy in national infrastructure through cyber-security measures and cyber-security is included as a top priority on the national security agenda. This means that measures that are generally regarded as being within the purview of information security may now also be included among measures to ensure national security and vice versa.

5. CONCLUSION

It is no doubt that using information and communications technologies has become widespread in daily life in the world today. As mentioned above, such new scenario of possibilities offers unprecedented development in the exchange of information and communications, but at the same time it entails serious risks and threats which can affect national security. Actually, given the complexity of existing vulnerabilities in cyberspace, it can be strongly accepted that moreover they have the potential to undermine the nations' confidence in the information systems that underlie economic and national security interests of the states.

Therefore, cyber security mainly focuses on protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible. As such, cyber security is a type of security much embedded into the everyday routines and technologies of actors who are not even necessarily professionals of security. However, this does not diminish the importance of cyber security measures and activities in the context of the overall efforts of the states in promoting and enhancing national security. In fact, such

situation and practice regarding to the cyber security providers further contributes to the reduction of firmly established boundaries between private/state, or civil/military discourse and approach in the analysis of the contemporary security environment.

The paper analysis shows that with the rise of cyber threats as well as the increase of insecurity in cyber space, the clear line between internal and external threats that states face today is increasingly being lost. In fact, the states as well as the international organizations, are increasingly faced with the reality of the existence of a new insecurity environment (cyber space), which imposes the need for the implementation of new approaches and instruments in the promotion of security. It is a positive aspect that such need is already recognized and that states and international organizations have already created strategic responses in promotion of cyber security.

As example, Spain adopted a National Cyber Security Strategy in 2003, while the Worldwide Threat Assessment of the US Intelligence Community put ‘Cyber and Technology’ as the top priority ahead of other prominent threats including terrorism, the proliferation of weapons of mass destruction and counterintelligence. Compared to a decade ago – and before – when cyber and technology were at the bottom of this list, this is an alarming development that begs significant attention (US Intelligence Community, 2016). In 2020, Australia has also adopted a Cyber Security Strategy, while in its most recent strategic document in the field of security and external activities (named as: A Strategic Compass for Security and Defence, 2022), the EU also recognizes the need for further developing of the Cyber Diplomatic Toolbox and for setting up an EU Cyber Defence Policy as an instrument for better preparedness and response to cyber-attacks (EU, 2022).

Such examples show that cyber security measures are increasingly being incorporated into the national security of states and hence into their efforts to create resilience especially of critical infrastructure from cyber-attacks. It is no doubt that strengthening the resilience of critical infrastructure simultaneously increases the resilience of society as a whole. As a result, within the contemporary security agenda, there is a new, so-called synthesized perception and understanding of the terms technical security and national security. Moreover, as a result of the new above-mentioned dynamics in cyberspace, it becomes practically impossible to consider these two types of security separately.

Of course, it does not mean that the protection of critical infrastructure and objects has not been part of the previous national security planning process, but that the nature of cyber threats (the advantages of their offensive capabilities in relation to defensive ones, problems with detecting the attack and the perpetrator, the challenges related to securing civil and national networks, as well as closing any vulnerability), necessarily imposes the need for analyzing and accept cyber security as part of the contemporary security agenda.

REFERENCES

1. A Strategic Compass for the EU (2022). European Union, online: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en
2. Buzan, B., Wilde, J. D., Waever, O., (1997). Security: A New Framework for Analysis. Lynne Rienner Pub.
3. Cavelti, M.D. (2007). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (1st ed.). Routledge.
4. Cavelti, M.D. (2010). Cyber-Security, in: The Routledge Handbook of New Security Studies, Burgess, P. (eds.), London and New York: Routledge.
5. Choucrist, N. (2012). Cyber Politics in International Relations. Cambridge: MIT Press.
6. Clarke, R. A., Knake, R. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins.
7. Cyber-attacks statistics (2020 and 2022). KonBriefing researcher, online: <https://konbriefing.com/en-topics/cyber-attacks-2022-cny-germany-q1.html>
8. Cybersecurity: main and emerging threats (2022). European Parliament Report, online: <https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats>
9. Cyber Security and Infrastructure Security Agency (CSISA) Report (2021), online: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>
10. Fischer, E.A. (2005) Creating a national framework for cyber-security: an analysis of issues and options. CRS Report for Congress, online <http://www.usembassy.it/pdf/other/RL32777.pdf>>
11. Nye, J. (2010). The Future of Power. New York: Public Affairs.
12. Rid, T., McBurney, P. (2012). 'Cyber-Weapons', The RUSI Journal, 157(1): 6-13.
13. Škanata, D. (2020). Improving Cyber Security with Resilience, in: Annals of Disaster Risk Sciences, Vol 3, No 1.
14. Valeriano, B., Ryan, C. M. (2015). Cyber War versus Cyber Realities. New York: Oxford University Press.
15. Worldwide Threat Assessment of the US Intelligence Community (2016). US Intelligence Community Report (2016), online: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf