Intrusions on State Digital Infrastructure in North Macedonia: Digital Human Rights Impact Analysis

By Oliver Risteski

DCAF *Young Faces* Participant 2022

Abstract

In our digital world, where cyber threats are increasing every day, making the identification and protection of critical digital infrastructure even more crucial for securing digital human rights and democracy. Intrusions against states' official websites have become common, the most notorious one in North Macedonia being the DDoS attack that happened on the day of last parliamentarian elections, which caused mistrust in the entire election process. This paper is focused on the protection of digital critical infrastructure, intrusions, and the impact on digital human rights. Implications on human rights can be serious if the state does not have good cyber security governance that protects rights, such as right of privacy and right of freedom of expression. Macedonian digital society has experienced many violations of digital rights. The most evident are cases where personal data stored in the state's official databases is breached and becomes public. This paper will utilize the case study of recent cyber-attacks to illustrate the challenges for North Macedonia.

Keywords: digital critical infrastructure, digital rights, cyber threats, DDoS attack, intrusions

Election day DDoS attack on the State Election Commission

We are living in an increasingly digitalized world, in which cybercrime poses a serious threat to individuals, society and the state. The need for the protection of the information society is of paramount importance for the maintenance of normal functions, safety, economy and well-being of the people. Damage or destruction of these systems can have a significant impact on fundamental human rights as well on the institutions of the whole state and democracy. At the same time, the critical infrastructure is an important and essential part of national security. The recent cyber-attacks have demonstrated the risks and damages that the critical infrastructure is exposed to. In order to protect the digital critical infrastructure, digital rights and property of citizens and institutions, responses must be rapid, coordinated and efficient. It should follow the basic principles of digital critical infrastructure protection, effective protection requires continuous communication and coordination of all relevant stakeholders, including time standards, constant exchange of risk assessments, threats and vulnerabilities of digital critical infrastructure.

The most notorious Distributed Denial-of-Service (DDoS) attack against Macedonian digital critical infrastructure happened on the day of the last parliamentarian elections. Early parliamentary elections in North Macedonia were held in July 2020. Shortly after the polls closed, the official website of the State Election Commission (SEC) was inaccessible to citizens. The President of the SEC, Mr. Oliver Derkoski, indicated that he was unaware of the causes of this incident.[1] This website is the main source for monitoring the election results and informing the citizen. At the same time, the biggest news aggregator time.mk, stopped functioning as well and the owner announced through Twitter that, so far, their Cloudflare had blocked 3M IP addresses. These incidents, led to the conclusion that the critical Macedonian digital infrastructure on the day of the parliamentarian election was under DDoS cyber-attacks. Macedonian citizens were in turmoil and chaos that night because there were no official results of the parliamentarian elections.

The fall of the SEC website revealed many other issues, such as cybersecurity and specifications of the web application and the procedure for procuring the application for the election results of the SEC. The day after the elections, media outlets reported that the procurement was disputable, as it was made without an open competition. The SEC only invited two companies for the procurement of new and upgraded software solutions: Duna Computers and I Vote, with the SEC selecting the former. IT company Duna Computers would implement secure software for the Parliamentarian election.[2] After the cyber-attack happened, the SEC immediately reported it to Duna Computers, the company responsible for the electronic system for entering and transmitting election statistics, thinking that the problem was in the application. Official reports from Duna Computers claim that the official website of SEC had crashed, but the page containing the election results was safe since it functions as a separate platform. Nevertheless, there was severe panic and chaos in the SEC, and no one knew what to do. Duna Computers claims that they tried to explain to the SEC that the problem was in their servers. The application where the election results are entered is placed in a separate network from the one seen by the public, independent of the SEC website, and is administrated by Duna Computers. This is separate from the SEC's own servers, which came into use around mid-2022. Although the SEC is subscribed to protection which should have quickly rejected this kind of cyber-attack and re - establish access to the site, this did not happen soon enough. After unsuccessful attempts from A1 North Macedonia to deal with the problem, the attack was stopped by the international telecommunications company A1 Austria after it noticed unusually high traffic per second.

Shortly after the end of the election process, at a press conference held by the SEC, the President of the organization, Mr. Oliver Derkovski, stated that the SEC was under a cyber-attack. Afterwards, the whole procedure for entering the votes digitally slowed down due to an avalanche of reactions when the SEC's official webpage was unavailable for hours. There was no access to obtain information on how the votes were counted, as was the practice from previous elections. The results were delayed, the ballots were counted manually, and the final results were shared with reporters via

[1] Blazhevski, Bojan "The Website of the SEC for the Election Results Fell, the Aggregator time.mk Under Cyber Attack."
[2] ECJH "Agreement for Procurement of New and Upgrading of Existing Software Solutions in the SEC" (Accessed April 19, 2022)

Google folders. Protection of the SEC's servers against DDoS attacks was administered by the well-known US company Cloudflare. The SEC's IT sector stated following the DDoS cyber-attack that due to the nature of the attack, their Cloudflare security system failed to detect the attack. According to the official answer of the submitted Freedom of Information Request to the SEC, on the day of the parliamentary elections in 2020, a DDoS attack was carried out targeting the official website of the state election commission, which contained the application for announcing the results of the conducted elections. They stated that there was no damage to the SEC, and only the publication of the official results of the parliamentary elections was prevented. Although the incident was reported to the Ministry of Interior, it has not yet been determined who carried out the attack and where it came from. When asked about specifics on their electronic systems, the SEC refused to provide such information, explaining that such information on their electronic systems was not for public procurement. When asked about the security of the server from the official website of the SEC, it stated that the IT administration of the SEC oversaw the overall administration of the official website.[3]

In terms of the security of the biggest news aggregator time.mk, owner Mr. Igor Trajkovski mentioned that, on the 15th of July 2020, it had two types of attacks on their website: one was a DDoS attack, and the other was an attack of unauthorized access. He pointed out the consequences in the media space, specifically noting distrust in the whole election process since the official website of the SEC where the election results were monitored was unavailable for several days. This was compounded by the fact that the most visited news site, which conveys elections results to many readers, was compromised for about 20 minutes. Mr. Igor did not know the perpetrator of these attacks, although he pointed out that there was an individual on Twitter who took responsibility and wrote with slightly unusual language in Macedonian. It was indicated that the attack on time.mk was not reported to MKD-CIRT, though it was reported to the Ministry of Interior. Unfortunately, it did not receive any answers, information or additional questions about the investigation. When asked about the protection of digital critical infrastructure in North Macedonia, Mr. Igor noted a recent number of frequent hackings, unavailability or dysfunctions, and defacement of state websites. Mr. Igor's recommendations for improving cyber security included improvement of protection at the national level and governmental employment of experts in the field.[4] The confusion and uncertainty which surrounded the election results could also be attributed to the fact that the State Election Commission did not have a standard protocol for what to do in this type of cyber-attack. In fact, it was only until the next day that it reported the cyber-attack to the police.

Allegations of election irregularities and party objections were overshadowed by the SEC cyber-attack. Within the scope of this paper, a freedom of information request to the Ministry of Interior regarding the intrusions against the system of the State Election Commission for displaying the voting results of the Early Parliamentary Elections 2020. The investigation was led by the Department of Computer Crime and Digital Forensics - Computer Crime Investigation Unit. It had conducted measures and activities in the scope of the criminal investigation. According to their criminal investigation the DDoS attack on 15.07.2020 started at 21.00 with lower intensity [SMR (PING request)] searches. This DDoS attack was used to suppress the State Election Commission's services to the external Internet (display of results through the official website of SEC https://rezultati.sec.mk/ to the general public), but not for unauthorized entry, unauthorized download of computer data or manipulation of data from the 2020 Early Parliamentary Elections.[5] Although the investigation conducted by the Ministry of Interior claims that the number of votes was not manipulated, it is important to note that the evening following the voting, Macedonian citizens were unable to have secure access to the official website of the SEC, preventing their right to be truly informed on the elections results by a reliable source. This led to mistrust in the entire election process.

Cyber-attacks against digital critical infrastructure: on the rise during the pandemic

Previously, Macedonian digital infrastructure was subject to multiple cyber-attacks. The Ministry of Interior has investigated several cases under Article 251 "Damage and unauthorized entry

[3] "SEC Resolution for Answer of Freedom of Information Request Reg. No. 03-703/2" (March 5, 2022)
[4] Email Correspondence with Igor Trajkovski, Owner of Time.mk" (2022)
[5] "Ministry of Interior Resolution for Answer of Freedom of Information Request Reg. No. 16.1.2-341/1" (March 14, 2022)

into a computer system" of the Criminal Code of the Republic of North Macedonia, which applies to systems of the government, ministries, local communities, government bodies, and state and educational institutions. In the past 2-3 years, the Sector for Cybercrime and Digital Forensics has seen an increase in reported criminal cases of this type, where DDoS computer attacks most often occur at times of important state processes, such as the census or elections. Impact includes further unauthorized access into computer systems and changes to the website of institutions, as well as launching viruses or intrusions with cryptocurrency and malware.

After analysing relevant submitted logs in relation to the computer attack, the Sector for Cybercrime and Digital Forensics concluded that the case with intrusion of the digital critical infrastructure of the Government of North Macedonia was an unauthorized entry into a computer system. The analysis concluded that the attack was carried out from foreign IP addresses. However, there are legal entities that offer Internet services to hide the identity of users of Internet IP addresses known as VPN / proxy servers.

During the COVID-19 pandemic, when the platform for online learning had just begun, there was another case of a DDoS computer attack on the subnet where the National Distance Learning Platform schools.mk was hosted. The investigation of the system logs had shown that there were two types of DDoS attack, the first an ICMP flood attack which the platform automatically blocks, and the second GRE based protocol which is quite massive in number of packets per second but does not create a significant volumetric amount of data. There is no fully automatic blocking technique, and its suppression requires regular coordination between the operational centres. In addition, due to the nature of this attack, it was not possible to obtain more detailed information about the IP addresses from which the attack was performed.[6] The Ministry of Education and Science denied the information that appeared in the media and on social networks, which suggested that an intrusion was made in the electronic systems and databases of the Ministry. According to its internal investigation, no intrusion into the electronic systems of the Ministry of Education and Science was detected. The Faculty of Information and Communication Technologies oversees the security of the Ministry's servers.[7]

In 2018, during the population census by Households and Dwellings, a DDoS attack was conducted against the website of the State Statistical Office (stat.gov.mk). Official reports of the State Statistical Office were submitted to the Sector for Computer Crime and Digital Forensics, which concluded that a DDoS attack was performed. It was an attack from many IP addresses that affected the availability and functionality of the website, and they had foreign VPN/proxy servers.

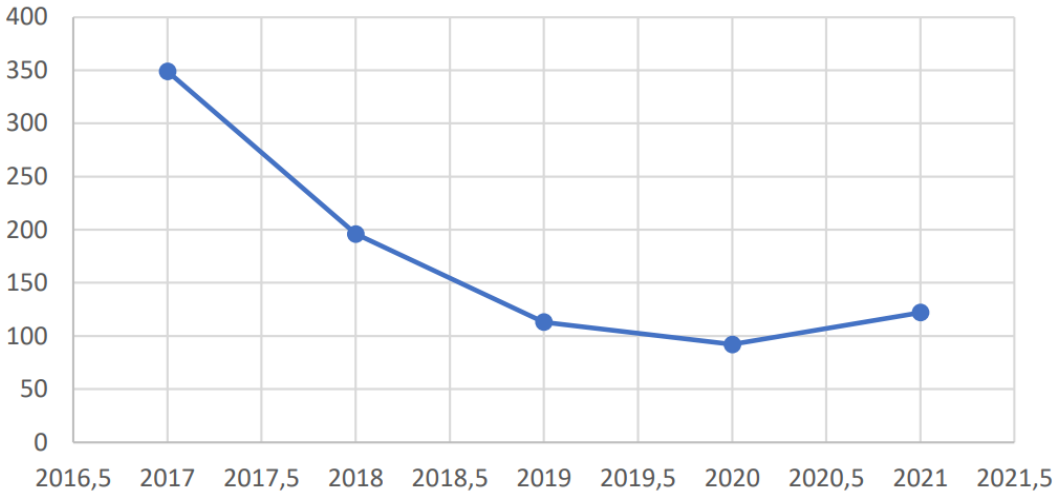
The National Centre for Computer Incident Response, MKD-CIRT, since its establishment within the Agency for Electronic Communications, adopts the legal framework that regulates the operation of MKD-CIRT. CIRT teams should have other legal responsibilities: monitoring incidents at the national level; implementing an early warning system; notifying on risks and incidents; performing risk and incident analysis, etc. There is no legal obligation for mandatory reporting of incidents in MKD-CIRT, so the reports are mostly on a voluntary basis, from stakeholders or third-party sources. Most of the reports are automatic periodic reports with cumulative information sent from abroad (other national CSIRT and international organizations), which investigate Macedonian public IP addresses, as either a source or a party to malicious activities abroad. MKD-CIRT periodically informs the providers about these allegations with a request for verification and informing the end user in case of confirmation of the allegations from the application. According to MKD-CIRT's available statistics from 2017-2021, in 2021 a total of 122 public websites were hacked, compared to 92 in 2020, 113 in 2019, 196 in 2018 and 349 in 2017. Out of these, the number that were official websites of organizations from the government sector under the gov.mk domain was eight in 2021, six in 2020, 24 in 2019, 24 in 2018 and 23 in 2017. The primary purpose of hacking is to change website content and hacktivism.[8]

[6] Ibid

[7] "Ministry of Education and Science Answer of Freedom of Information Request Reg. No. 03-3724/2" (April 5, 2022)

[8] "MKD-CIRT Answer of Freedom of Information Request Reg. No. 2101-1260/2 and 2101-1261/2" (April 21, 2022)

Numbers of hacked Macedonian public web sites by year



What is DDoS or Distributed Denial of Service Attack?

There are various computer attacks, but DDoS attacks have one purpose: to burden the system with requests to access the server. It happens when hackers try to flood the servers behind the website that is the target of the attack, in order to create as much traffic as possible until the website becomes inaccessible to users. DDoS attacks usually work through a network of bots, which are a large group of distributed computers that act together to spam a website or service provider from which they request data.

Usually, cyber-attacks get into the server to make certain changes or download data. DDoS attacks can disable the websites of the critical infrastructure or, as it is popularly called, “push it.” This is done to disable a particular website in order to prevent access to users' services. The second goal is to create chaos or confusion so that another operation can be performed in the background, which was the case during the Macedonian parliamentary elections.

A DDoS attack, by its technical nature, does not constitute a criminal act of unauthorized entry into a computer system, as it only effects the availability of services delivered over the Internet. But this type of attack can cause large damage when it comes to the availability of digital critical infrastructure during important events, such as elections, censuses, etc. As these events should be safe and reliable, their unavailability strikes a blow to the trust of the institutions of the state and its democracy.

DDoS attacks can be bought or ordered from the Internet, specifically on the dark web. In April 2018, a website that sold DDoS services, Webstresser.org, was frozen and the administrators charged with cybercrimes thanks to an international investigation led by the Dutch National High-Tech Crime Unit and the UK National Crime Agency, with the support of many other organizations. Operation Power Off is just one example of how international actors can work together to create a more secure cyber environment for users.[9]

DDoS defense systems

Many cybersecurity systems protect network resources through preventive and reactive activity levels, deployment location and degree of required cooperation with other network mechanisms and services. Reactive mechanisms differ in attack response strategies, including sources or flow packet dumping, routing reconfiguration and attack rate-limiting. However, in general

[9] DCAF “Guide to Good Governance in Cybersecurity, International Investigation” p.32

the efficiency of attack mitigation depends on packet filtering methods and their efficiency. The most significant challenge is separating the attack from legitimate traffic and implementing responses tools in the network environment. In general, the detection is based on pattern matching algorithms. A flow consists of pockets that match conditions describing packets attributes, such as IP source and destination addresses, sources and destination port number or protocol. Malicious detected flow is redirected to a scrubbing center to be cleaned from malicious components. The standard model of DDoS protection is based on managed security services delivered by ISPs or DDoS Protection Service providers.[10]

Human rights in digital age

The digital transformation of our society is certainly one of the fastest and most profound transitions of civilization we have ever experienced. This digital age is leading us to interact more and more online for information, entertainment, consumption and work. Human rights, such as the right to freedom of expression, right of privacy and the right of safe access to information, have long been very relevant in our daily lives, but the increased use of digital technology and the development of e-government brings these debates even more into the limelight. Digital technology is evolving very fast, bringing many benefits, but on the other hand many new forms of cyber threats that can jeopardize cyber space and digital human rights, such as freedom of expression and access to correct and trustworthy information. Under Article 19 of the International Covenant on Civil and Political Rights, "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[11] It becomes self-evident that the cyber security governance must be better regulated and implemented by all the stakeholders in the state in terms of national and international level, because cyber-crime does not have frontiers. The rise of DDoS attacks and intrusions that targeted digital critical infrastructure of North Macedonia, particularly during the critical events of parliamentary elections and census, undermine democratic norms which guarantee fundamental human rights. Digital infrastructure in North Macedonia has often been the target of attacks by various perpetrators, some of them taking liability by posting on Twitter. Some of these attacks were directed at state webpages on whose servers personal data of Macedonian citizens are stored. Many media outlets have published articles claiming that Ministries and others state entities were also targets of cyber threats, supported by instances of unauthorized entrance into state servers and personal data breaches. For example, the Ministry of Healthcare faced a data breach whereby medical records and whole personal profiles of Macedonian citizens, which were stored on the Ministry's servers, were targeted. Afterwards, the perpetrators published the official database of personal email addresses as proof on Twitter.[12] As a reminder, personal data refers to any information related to an identified or identifiable natural person, like email addresses are personal data, as they usually contain an individual's first and last name and where they work. If one is able to identify an individual either directly or indirectly, even in a professional capacity, such data is personal data. According to the General Data Protection Regulation (GDPR) under Article 4(1) "personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or connected to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) both provide that everyone has the right to the protection of personal data concerning themselves.[13] Share Foundation and Balkan Investigative Reporting Network (BIRN) have monitored the Balkan region's digital rights and freedom violations, and have registered many different forms of digital rights violations. The most notorious are publishing information about private life, computer fraud, illegal interception of electronic

[10] Niewiadomska-Synkiewicz, Ewa et al., Cybersecurity Resilience in Digital Society – the Practical Approach; Internet and New Technologies Law
[11] United Nations Human Rights Office of the High Commissioner "International Covenant on Civil and Political Rights"
[12] [@MkdOps]. "Emails database with personal data of all employees in the Ministry of Health"
[13] European Union "Regulation 2016/679, General Data Protection Regulation"

communications, illegal personal processing, publishing falsehoods and unverified information, insults and unfounded accusations, threatening content and endangering the security, hate speech and discrimination, creating fake accounts and paid promotion of false content, misinformation and other manipulation in the digital environment.[14]

If state digital infrastructure and personal data which are stored by the state are safe, does that mean the state has good cybersecurity governance? If we have no rule of law in the virtual world, how we can have rule of law in reality? These are very debilitating issues which require including all stakeholders, implementing all measures which are encompassed by the international and national legal framework, National Cybersecurity Strategy and Action Plan. International norms encompass universal values applicable to every human being. The Universal Declaration of Human Rights (UDHR) and European Convention on Human Rights (Council of Europe) bind states to actively engage in securing the enjoyment of human rights in the digital age. It means states must take active measures to protect their citizens against human rights abuses both offline and online. All countries from the Western Balkans region, including North Macedonia, have yet to adopt the GDPR, but if any organization in these countries collects data in the EU member states, they are bound by the GDPR. In the case of North Macedonia, where official state webpages were targeted and the right of privacy was breached, highlights the necessity for the state, alongside all other stakeholders to facilitate the enjoyment of basic human in the virtual world as well as in reality, and to build resilient information ecosystem and ensure protection of the digital rights and rule of law to our decentralized digital world.

Conclusion

From the cases presented in this paper, including several cyber-attacks in a relatively short period, most of them against official state webpages which store the personal data of Macedonian citizens, it is evident that Macedonian digital critical infrastructure is not adequately protected from these kinds of cyber threats and resulting digital rights violations. The climax of these cases was the case of the attack against SEC on the day of the parliamentary elections, resulting in turmoil and chaos in the media and for Macedonian citizens who even now are wondering what exactly happened on the 15th of July 2020. Even today we have no clear evidence of who was behind this cyber-attack, as the official investigation has not yet determined the perpetrator. Evidently, Macedonian law enforcement and all other entities, including MKD-CIRT and the IT sector of the SEC are not sufficiently equipped to investigate these incidents. These cases portray that risk assessment and resilience of Macedonian digital society must be enhanced with highly trained professionals in the field of cybersecurity and an overarching approach from all stakeholders. According to the Global Cybersecurity Index, North Macedonia is 38th place in the ranking out of 182 countries in the world. This ITU report highlights especially the technical limitations when it comes to cybersecurity.[15]

In the digital world where cyber threats are continually increasing, implications on the violations of human rights can be fatal if the state does not have adequate cyber security governance to protect rights like the right of privacy, and right of freedom of expression in digital terms. Recently, there have been many registered violations of digital rights. Illegal interception of electronic communications was notorious five years ago, as well as misuse of personal data (case Telegram-Public room), dissemination of racist and xenophobic material through computer systems, publishing falsehoods and unverified information deliberately, insults and unfounded accusations, threatening content and endangering the security, hate speech and discrimination, creating fake accounts and paid promotion of false content, misinformation, illegal access into computer systems and other manipulations in the digital environment. The level of media literacy is one of the lowest in the region, and the region is susceptible to external influences through misinformation, fake news and violations of digital rights. Research has shown that personal data which are stored on the servers of state institutions are critically vulnerable and easily targeted. Resilient information systems, risk assessment, and identification and protection of critical digital infrastructure must be enhanced. Vulnerability of personal data seems to be due to a lack of understanding and acknowledgment for good cybersecurity governance and protection of fundamental human rights, which are guaranteed by

[14] B.I.R.D. "Registered Digital Rights and Freedom Violations in North Macedonia"
[15] International Telecommunication Union "Global Cybersecurity Index 2020"

international treaties. What is especially missing in the legal framework is clear provisions related to the safeguards of fundamental human rights in digital terms, as well as the pressing adoption of GDPR and harmonization with EU legal frameworks.

Recommendations

The protection of fundamental human rights, personal data and privacy are essential principles. Digital rights are inherited fundamental human rights. Cybersecurity can be efficient only if based on fundamental rights and freedoms pursuant to the Charter of Fundamental Rights of the European Union and universal values of the EU. Thus, the rights of individuals cannot be ensured without having safe information systems. Having taken into account the lack of sufficient protection of both identity and digital critical infrastructure of state entities which store personal data, it is critical to undertake serious steps in order to protect digital rights. Considering the findings in this paper for the recent cyber-attacks against digital critical infrastructure and infringement of digital rights, the following non-exhaustive list of recommendation is proposed propose to various stakeholders to enhance cyber security governance and protection of digital rights:

To the Representatives of National Council for Cybersecurity:

The existing National Council for Cybersecurity should collaborate more with other similar agencies in neighbouring countries and the EU broadly to develop and adopt best practices in cybersecurity governance through twinning and exchange programmes. They should also seek better coordination and cooperation with domestic states and non-states entities as private companies, CSOs, academia, international institutions, etc. Implementation of the National Strategy for Cybersecurity (2018-2022) and action plan in this period has been lacking due to many missed planned activities which encompass the Strategy and Action plan that are yet to be implemented. When it comes to digital critical infrastructure, writing necessary procedures and processes for the identification of digital critical information infrastructure, as well as development and implementation of mandatory minimum-security protocol and continuously supervising such protocols must also be achieved.

To the Ministry of Education and Science:

Implementation of training for cybersecurity, media and digital literacy into school and university curriculums is important. This should promote the role and importance of cybersecurity certification in the IT field. Professional protection and highly trained experts must engage in protecting servers which store personal data and should implement the best IT solutions for cyber security, including possible regulations such as minimum requirements for the IT sector in any entities which identify as digital critical infrastructure. These activities pertain to the introduction of cybersecurity curriculums in elementary schools, high schools and institutions of higher education.

To MKD-CIRT:

Enhancing risk management in digital infrastructure, and developing standards, guidelines and procedures based on best international practice, must be implemented in the protection of digital rights. This includes development and approval of risk analysis procedures concerning security for the systems of national bank, commercials banks, public administration and other state entities which contain personal data. Other important dimensions are preparedness and resilient information ecosystem, ensuring fast down-time recoveries and continuity of normal functioning in cases of cyber-attacks. Awareness campaigns for employees in the IT sector should be developed, for both the public and private sector. Coordination and cooperation should be enhanced with all stakeholders, states, non-state, civil society and academia, including the employment of experts in the field of cybersecurity on appropriate IT sectors in each entity.

To the OSCE Mission in Skopje:

Active involvement of the OSCE Mission in Skopje in tackling cybercrime and modern forms of cyber threats against critical digital infrastructure is important, as is involvement of Macedonian law enforcement in the training process alongside experts in cyber security. Organizing seminars,

exercises and trainings for employees in the IT sectors of state entities and using the best practices in the protection of digital rights should be carried out.

To NATO:

Considering that North Macedonia is a member of the NATO alliance, the state must refer to the case in Estonia after the cyber-attack in 2007. Specifically, there should be a focus on its experience in research, development and protection of the digital critical state infrastructure. Furthermore, officially submitting a request to NATO for cooperation with the NATO Cooperative Cyber Defence Centre of Excellence must be considered. The establishment of a state body within the Ministry of Defense, specialized for cyber defense, which would bring together experts in cybersecurity from the government, military and academia must also be considered.

To Civil Society Organizations:

It is important to engage the wider community of civil society organisations, digital rights defenders and technology experts to further develop awareness campaigns of cyber threats and protection of digital rights, with the further aim of establishing an independent platform, Computer Incident Response Center for Civil Society.

Bibliography

[@MkdOps]. “Emails database with personal data of all employees in the Ministry of Health” Accessed April 2022

B.I.R.D. “Registered Digital Rights and Freedom Violations in North Macedonia” (Share Monitoring: Accessed April 2022)

Blazhevski, Bojan “The Website of the SEC for the Election Results Fell, the Aggregator time.mk Under Cyber Attack.” (Meta.mk, 2020)

DCAF “Guide to Good Governance in Cybersecurity, International Investigation” (Geneva, 2019) p. 32

ECJH “Agreement for Procurement of New and Upgrading of Existing Software Solutions in the SEC” (2020)

European Union “Regulation 2016/679, General Data Protection Regulation” (Official Journal of the European Union: Accessed June 2022)

International Telecommunication Union “Global Cybersecurity Index 2020” (Accessed June 2022)

Niewiadomska-Synkiewicz, Ewa et al., Cybersecurity Resilience in Digital Society – the Practical Approach; Internet and New Technologies Law (Baden, Nomos: 2021) p. 421

Risteski, Oliver “Email Correspondence with Igor Trajkovski, Owner of Time.mk” (2022)

Risteski, Oliver “Ministry of Education and Science Answer of Freedom of Information Request Reg. No. 03-3724/2” (April 5, 2022)

Risteski, Oliver “Ministry of Interior Resolution for Answer of Freedom of Information Request Reg. No. 16.1.2-341/1” (March 14, 2022)

Risteski, Oliver “MKD-CIRT Answer of Freedom of Information Request Reg. No. 2101-1260/2 and 2101-1261/2” (April 21, 2022)

Risteski, Oliver “SEC Resolution for Answer of Freedom of Information Request Reg. No. 03-703/2” (March 5, 2022)

United Nations Human Rights Office of the High Commissioner “International Covenant on Civil and Political Rights” (1966, accessed June 2022)