Prof.dr Tamar Kupreishvili

Georgian Technical University
Faculty of Law and International Relations

E mail: t.kupreishvili@gtu.ge

DOI:

Research Paper

Received: October 2, 2021

Accepted: November 10, 2021

NATO's Global Challenges and Russia's Cyberspatialities

"A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all"- NATO Secretary-General, Jens Stoltenberg

Abstract: Information became more important than material or energy resources in the XXI century. Resources are generally defined as community-owned economic potential elements that can achieve specific goals in economic activity. For modern society, material, financial, labor, natural resources became commonplace. Estonia was the first state in Europe to carry out a massive cyber-attack in April and May 2007. That was why the states decided to get the first convention to defend their cyberspace as they defended their land, air, and sea spaces.
In the XXI century in cyberspace, there are some main actors: The United States of America, Russia, Iran, China, North Korea, Israel. Russia is one of the most vital states in cybersecurity, which is constantly developing its abilities. The country has constant interests and goals for which he actively uses information space parallel with political and military opportunities.

Keywords: *Russia, NATO, Cybersecurity, CISA, Estonia*

INTRODUCTION

The concept "Information Resource" has also become commonplace, defined in the literature as information resources are separate documents, documents, and arrays of documents located in information systems (libraries, archives, databases, etc.). Information resources are the property of anyone or the organizations; they need to be registered and protected because information can be used not only for goods and services but can also be converted into cash, sold to someone, or can be destructed.

For an entrepreneur, owning information is of great value, as they often receive data that is a time-consuming and costly process. The term "Information" is defined differently in the different sciences. For example, in philosophy, information is defined as material objects and processes to store or generate certain conditions transmitted from one thing to another in the various subjunctive-energetic forms. In cybernetics, information is defined as uncertainly Elimination size.

The development of information technology and its penetration into all areas of human activity has given rise to the problem of information security. However, each year this problem becomes more and more complicated. Information Processing technologies are constantly evolving, with their increasingly changing and improving practical information security methods. The universal methods of information protection are not known; the construction of security mechanisms for the actual system largely depends on the individual characteristics of the system.

Information Security is seen as a set of information recommendations for building this or that type of information protection system. Practical steps in creating a protection system and the methods are based on such general patterns that are familiar and not dependent on specific technical realization. Such available practices and principles will be studied by a science called Information Security. Different states and organizations take other measures for information security, which is the continuous chain. The most vulnerable sectors are the financial institutions, banking sector; stock exchanges; nuclear power plants; water supply and treatment systems; personal data, e-government. Dimensions of cybersecurity are the following levels: political, military, economic, technical, civil society, and the citizens. The first steps of the violations in cyberspace appeared at the end of the 20th century, in the Gulf war, then in the conflict of Kosovo.

States decided to get a new convention about the defense of cyberspace, and the first convention was Budapest Convention on Cybercrime in 2001. The convention is the first international treaty on crimes administered via the web and other computer networks, dealing mainly with patent infringements and violations of cyberspace. Georgia joined this convention in 2008 but entered into force in 2012. (Convention on Cybercrime, 2001, p. 1-2)

Estonia was the first state in Europe to carry out a massive cyber-attack in April and May 2007. The hackers unleashed a wave of cyberattacks that crippled dozens of government and organizational corporate sites. The online attack followed Estonia's decision to move a Soviet World War II memorial from downtown Tallinn in April, where got protests from Russia's government and rioting among Estonia's ethnic Russian minority. The experts said that thousands of computers were used against the government and other sectors' two-phase attacks. The second phase is based on botnet attacks (DDoS attacks).

The Estonian government organized the international supporting process with international collaboration, mainly in politics. Estonian government framed DDoS attacks as a security point caused by Russia, and the western media and governments paid close attention to these two-phase attacks. On the international operations, Estonian internet security experts collaborated with the global internet security operations community and CERTs in other countries, including Finland, Germany, Slovenia, and other Baltic Sea countries. (Schmidt, 2013, p. 25)
Further massive attacks were carried out on Lithuanian cyberspace and the Georgian media space by Russia in 2008. Experts called it "Information War" against Georgia.
In 2011-2014 permanent cyberattacks were carried out by Russia on the United States defense and security of the structural subdivisions. The Pentagon and the National Security Agency (NSA) Departments were among them. During these cyberattacks was used the malware "Uroboros," which the first statement was made by the German security company "G Data Security" (G DATA, 2020, p. 2)

The following massive attack was on the Bank sector, concretely on the Bank JPMorgan Chase & Co. This source also was coming from Russia. In the XXI century in cyberspace, there are some main actors: The United States of America, Russia, Iran, China, North Korea, Israel. Russia is one of the most vital states in cybersecurity, which is constantly developing its abilities. The country has constant interests and goals for which he uses information space parallel with the opportunities of political and military actions. Russia started a complex approach to the issue, which means any military or other facial activities (social, political, economic), including the cyber-attack operations. (Svanadze, 2015, p. 31)

But not only states are actors, but several different actors know how to choose targeted and treat groups, use threat techniques, etc. To explain concretely, there is every year's FireEye report, which clearly shows how changed actors and their targeted groups depending on the situation in the world. For example, during Covid-19 research, the most targeted groups were schools and remote works. (FireEye, 2021, p.63) FireEye's report 2021 shows how the incidents are detected by percentage. These are divided into two groups: Internal Detection (when an organization independently discovers it has been compromised) and External Detection (when an outside entity informs an organization it has been compromised).

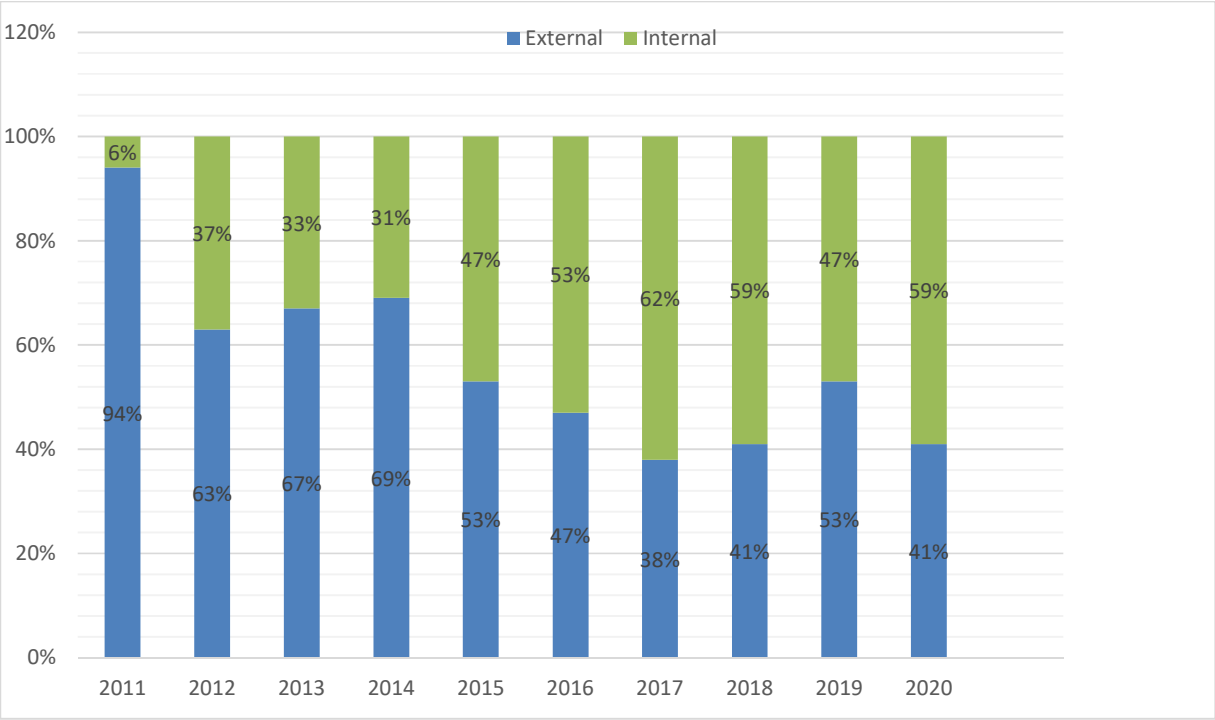

Diagram 1. Detection by source, 2011-2020:

According to the FireEye report, the top five most targeted industries were business and professional services, retail and hospitability, financial, healthcare, and high technology in 2020. It is clearly shown in diagram 2.

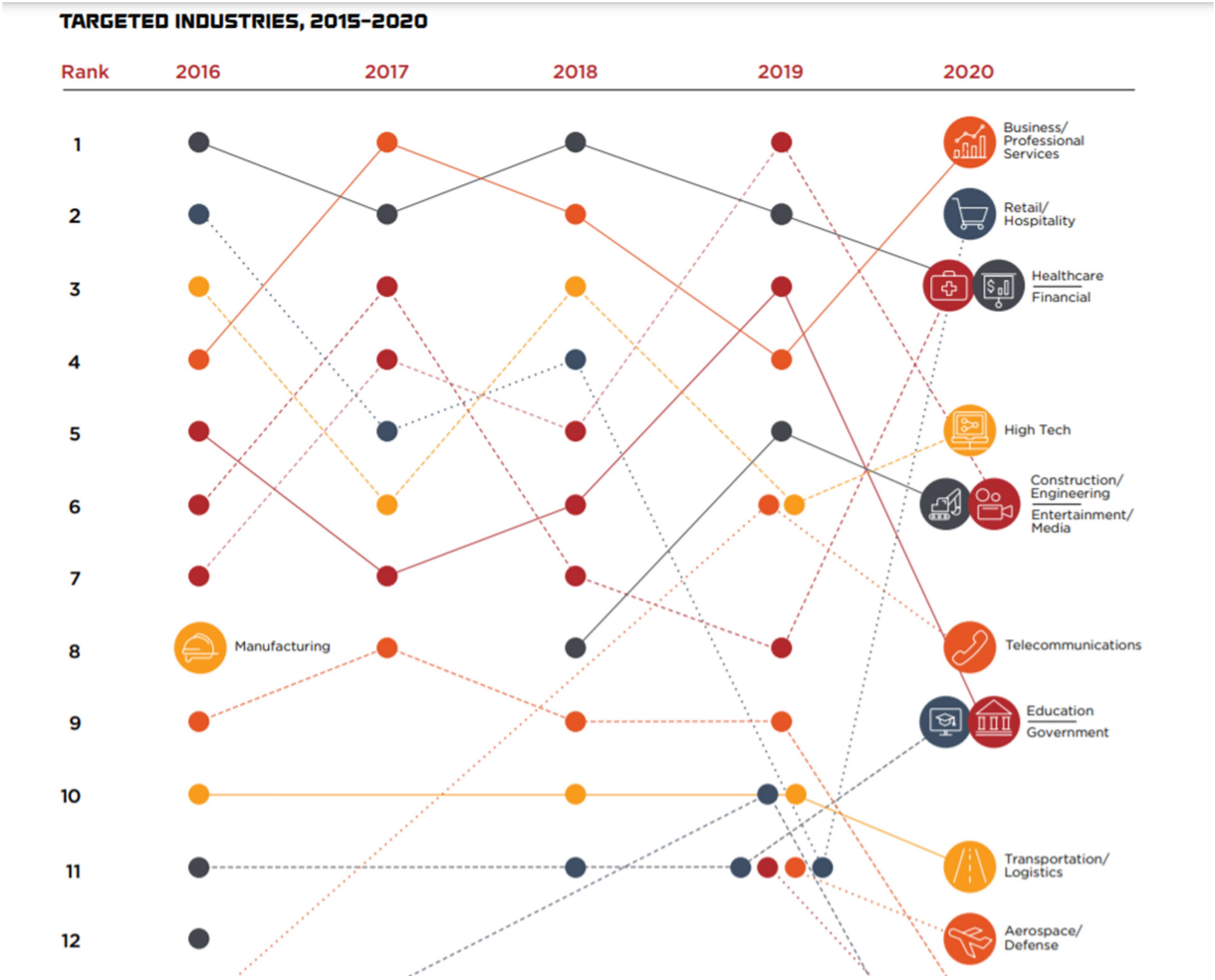

Diagram 2. The most targeted industries, in 2015-2020

According to the FireEye report, the most targeted attacks identified were exploits, phishing, and others (for example, brute-forcing). Their objectives were financial gain and data theft. (See the Diagram 3.)

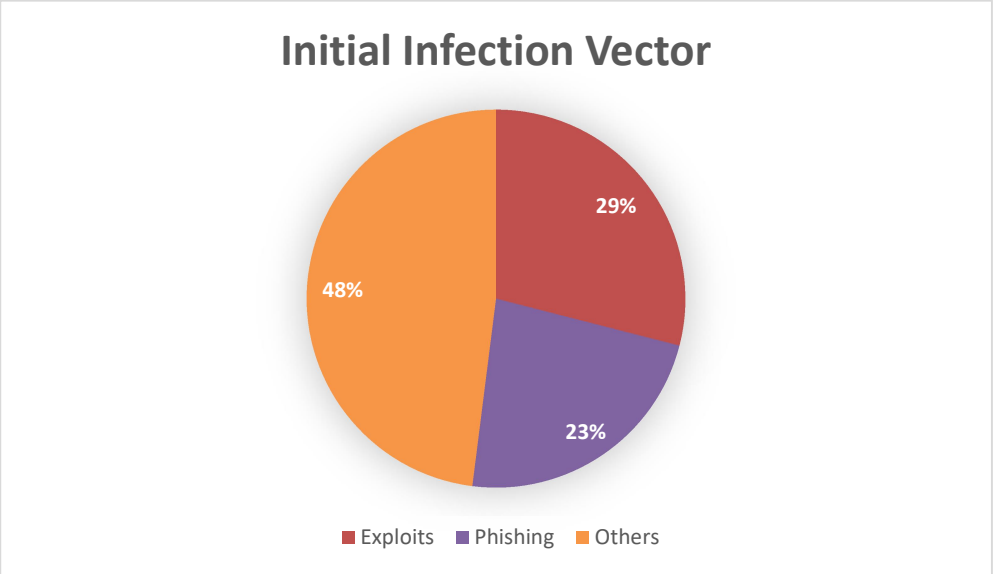

Diagram 3. Initial Infection Vector

During the sharing of information, the experts began tracking more than 500 new malware families. The malware family is a program or set of associated programs with sufficient "code overlap" among the members. (FireEye, 2021, p.67) The malware category distribution remains relatively consistent year over year. There are found top five categories: backdoors, downloaders, droppers, launchers, and ransomware. (See Diagram 4.)

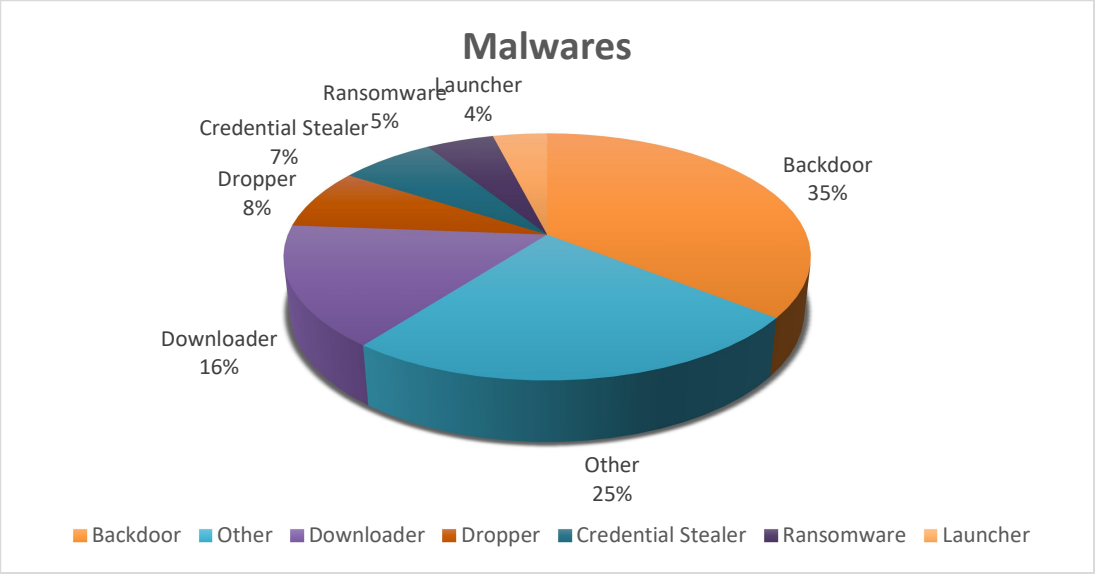

Diagram 4. Newly Tracked Malware Families by category, 2020.

If we compare the data of recent years, we will see that in 2020 both the cases and the financial loss were the highest. (See diagram 5.) (Cyber Attack statistics, 2021, p. 3)

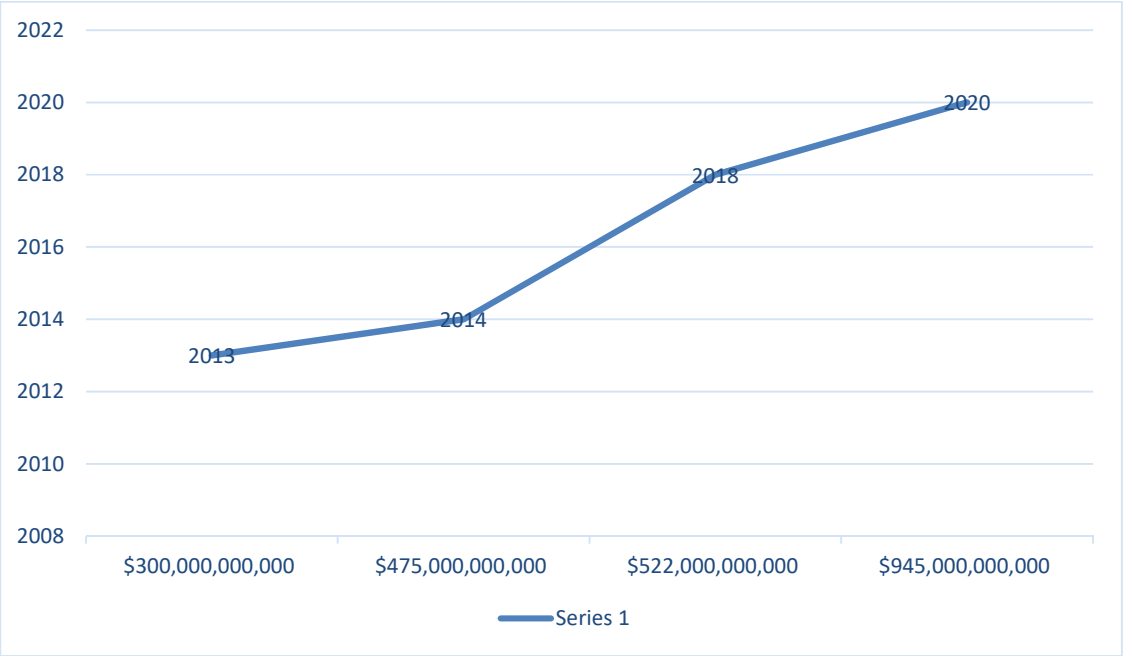

Diagram 5. General Cyber Attack Stats

From 2017 to 2021, the world has had different hacking incidents. Here are some (not complete list):

1. March 7, 2017 – 8761 documents have been stolen from CIA, iOS, and Android vulnerabilities, bugs in Windows (Published WikiLeaks and called "Vault 7").
2. June 19, 2017 – 198 Million US voter records exposed.
3. May 2017 – Macron Campaign Hack (Wired, 2017, p. 3))
4. September 6, 2018 – 380 000 travelers' plane tickets, their data, and complete credit card information were stolen from the company of British Airways. (Sandle, 2018, p.4)
5. November 2018 – 500 million hotel guests' information had been stolen from Starwood Hotel. (Bluefin, 2018, p.1)

In 2019, the world had the five most significant and notable cyberattacks:

1. American Medical Collection Agency affected 25 million included personal and financial data, social security numbers, medical information.
2. Citrix Systems, Inc. There is not shown the number of victims, but the stolen information includes names, social security numbers, financial information. The company thinks the hack resulted from the "password spraying" technique.
3. Capital One – Affected 106 million, included customers' credit card information.
4. Facebook, 419-540 million affected, included unique FB IDs, phone numbers.
5. First American – 885 million records, involved mortgage documents, personally identifying information, bank account numbers, driver's licenses, Social Security numbers, tax records, and others…. (Gordon Flesch Company, 2019, p. 5)

In the first half of 2020, 445 million cyber-attacks occurred. (Cyber Attack statistics, 2021, p. 11) But in the other half of 2020, the most crucial cyberattack was the United States federal government data breach by a group backed blamed the Russian government, where were penetrated thousands of organizations globally included multiple parts. Distressed organizations included NATO, the U.K government, the EU Parliament, Microsoft, et al.

The first affection was known from the U.S. Treasury Department and the National Telecommunications and Information Administration, part of the United States Department of Commerce. CISA (Cybersecurity and Infrastructure Security Agency) acknowledged that the hackers used "tactics, techniques, and procedures that have not yet been discovered." The bang has been "isolated to business networks" and "has not banged the mission-essential national security functions of the Department, consisting of the National Nuclear Security Administration," which oversees the nation's stockpile of the nuclear weapons.

A GAO Director on the IT and Cybersecurity Team, Vijay A. D'Souza said: "Even if everything was highly efficient within the state's cybersecurity, it's quite likely this breach wouldn't be caught." (Cohen, Fung, Marquardt, 2020, p. 2) Pompeo marked this cyberattack as "The Mark Levin Show," and Reuters first reported the hacking. In his first comment, Trump said it could be China instead of Russia.

Then, the Trump administration prepared a report that a group backed by a foreign government carried out a cyberattack. Two weeks later, US officials believed that Russia was responsible for that attack, but the Russian embassy in Washington denied this involvement in the hacking. (Stracqualursi, Liptak, Hansler, 2020, p. 8) In 2021, a major cyberattack has forced to shut down the gas pipeline in the United States of America that supplies 45% of all fuel consumed on the East Coast. This is a ransomware attack. This pipeline transports 2.5 million barrels of gasoline, diesel, and jet fuel in a day through 5.500 miles of pipelines…

The federal government actively works to find who is back to this attack, and on May 11, 2021, F.B.I identified who was back to this process, the hackers' group called Dark Side. (The New York Times, 2021, p. 1) The first news was confirmed by cybersecurity firm FireEye about this attack. (Stoltenberg, Dean, 2019, p. 19) As for the United States, other states, and International Organizations, cyberattacks play an essential role today, especially in the pandemic period.

CONCLUSION

Finally, to keep safe, NATO has been doing it for 70 years but now trying to adapt to this new reality. At the 2016 Warsaw Summit, the states unanimously recognized that cyberspace is as necessary to protect as the sea, the land, and the air, which is why it was named the Fourth Space. NATO developed prospects about cyber resilience, how to guard against the great security threat of the 21st century. In this prospect, there are some major topics on defending cyberspace. (Stoltenberg, Dean, 2019, p. 21) The XXI century is very active in cybersecurity, especially in 2020-21 years, depending on the Covid-19 Pandemic. Cybercriminals have been given more opportunities as the pandemic has made the world largely depend on the Internet.

References

Council of Europe., (2001). Convention on Cybercrime, Budapest Convention, Council of Europe Full list (coe. int)

Schmidt Andreas., (2013). "The Estonian Cyberattacks", Delft University of Technology.

G DATA., (2020). Digital security for your successful future, "The best G DATA of all-time" (gdatasoftware.com)

Gotsiridze A. Svanadze v. (2015) “Cyber defense”, Georgia

Fire Eye, M-trends, (2021). "special report" USA https://content.fireeye.com/m-trends/rpt-m-trends-2021

M-trends, FireEye, (2021). USA https://content.fireeye.com/m-trends/rpt-m-trends-2021

2021 Cyber Attack Statistics, Data, and Trends, (2021). 2021 Cyber Attack Statistics, Data, and Trends | Parachute (parachutetechs.com)

WIRED, (2017). "The Biggest Cybersecurity Disasters of 2017So Far", wired.com

Sandle, P., (2018). "BA apologizes after 380 000 costumers hit in cyberattack", Reuters

Bluefin The Leader in Payment Security., (2018). "Cyber Attacks In 2018: Biggest Cyber Security Data Breaches of 2018" (bluefin.com)

Gordon Flesch Company inc., (2019). "Cybersecurity - 5 Biggest Cyberattacks of 2019 and Lessons Learned" (gflesch.com)

2021 Cyber Attack Statistics, Data, and Trends., (2021) Parachute (parachutetechs.com)

Cohen Z., Fung B., Marquardt A., (2020). "US cybersecurity agency warns suspected Russian hacking campaign broader than previously believed", CNN US cyber-attack: Cybersecurity agency warns suspected Russian hacking campaign broader than previously believed – CNN Politics

Stracqualursi V., Liptak K., Hansler J., (2020). "Trump Downplays massive cyber hack on the government after Pompeo links attack to Russia"., CNN Cyberattack: Trump downplays massive cyber hack on the government after Pompeo links attack to Russia – CNN Politics

The New York Times., (2021). "F.B.I Identifies Group Behind Pipeline Hack", USA https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html

Stoltenberg Jens, Dean Alex, (2019). Prospect, "Cyber Resilience", 2019