When Digital Attacks Turn Physical: National Security in the Age of Cyber Threats

Akaki Shekeladze

PhD (Management), Associate Professor, Georgian American University, Tbilisi, Georgia.

Email: *akaki.shekeladze@gau.edu.ge*

Abstract

Cyber attacks are usually aimed at compromising personal, business or state sensitive information and IT systems, either for gaining access to data, finance or performing online sabotage. The world has seen various examples of cyber attacks affecting everyday life, from delaying or cancelling multiple flights to the destruction of physical infrastructure. The paper explores the growing interconnection between cyberspace and the physical world, emphasizing how cyber incidents targeting critical infrastructure, such as healthcare facilities, energy systems or transportation networks can directly endanger citizens' safety and disrupt national resilience. The reader will have an overview of the key challenges in the cyber space, which is an alarm for the national security. The text analyses various cyber attacks which managed to affect citizens' physical security and pose serious threats to the overall security of the countries. Emphasis will be made on the nature of the modern cyber space and how malicious actors adapt to changes in the world, demanding both private and state sector to be cyber aware and alert to avoid becoming victims. The research highlights the current vulnerabilities and makes prognosis for the future, how and why cyber attacks can cause even more danger to everyday life. Moreover, information will be provided about the possible solutions, based on the foreign experience, research data and statistics. The study concludes that safeguarding national and citizen security in the 21st century requires not only technological adaptation, but also strategic foresight and coordinated governance at all levels, in all sectors.

Keywords: Cyber Security, Cyber Attack, Sabotage, Hackers, National Security, Civil Safety

Introduction

The recent history of the world includes large-scale cyberattacks carried out in the 21st century, most of which are attacks against states. Attacks are carried out using such tools and technical means as: social engineering, phishing, DoS and DDoS attacks, malicious programs including Ransomware, Spyware, as well as Zero-Day exploits, etc. In the wake of the development of technologies, hackers try to strengthen their capabilities, which includes the development of their human resources, as well as the refinement of tactics, and the strengthening of software tools in order to be able to successfully achieve the malicious goals they set.

This paper discusses the most powerful and well-known cyberattacks carried out against the states. It is about those software tools and technical potential that create the basis for alarm in modern cyberspace and represent the greatest risk for the information security system of the world governments. The results obtained as a result of the research concern not only information systems, but also physical infrastructure. Innovative means of preventing the mentioned threats are proposed and further stages of the research are set to assess their practicality, applicability, feasibility and effectiveness.

Main Body

1. Destruction of Physical Infrastructure Using Cyber Means

Today, software and non-software means are distinguished from the types of cyberattacks. Even in the last century, there were cases when not only information systems were damaged by software and hardware, but also physical, real infrastructure.

Below are some notable examples of these cases, depending on the means used.

1.1.Trojan.

It is well known that in the 21st century, opposing countries no longer use classical methods of war to achieve their malicious goals. However, in as early as the 80s of the last century, there was a case when cyber activity damaged physical infrastructure.

The first such incident was on the Urengoy-Chelyabinsk gas pipeline in June 1982, where an explosion with a capacity of three kilotons of TNT equivalent occurred using a Trojan. It is noteworthy that no more powerful non-nuclear explosion has been recorded to date. The Trojan Horse software, which was intended to automate technological processes on the gas pipeline, secretly contained a so-called "logic bomb". Its essence was that the program correctly executed several hundred thousand cycles, and then changed the output parameters, which, in turn, increased the pressure in the gas pipeline twice [11].

1.2.Virus.

On August 5, 2008, an explosion occurred on the Turkish section of the Baku-Tbilisi-Ceyhan oil pipeline near Refahiye. According to information security experts, Russian special services were responsible for the explosion. The pipeline network was allegedly hacked through a surveillance camera. The hackers disabled alarm systems and increased pressure, causing an explosion. As a result, 30,000 barrels of oil were spilled, causing BP and its partners to lose $5 million and Azerbaijan to lose $1 billion in revenue [12].

1.3.Virus (Worm) and Zero-Day Exploit.

Most of the public is familiar with the rather large-scale and powerful cyberattack carried out in 2009-2011 by the worm “Stuxnet”. A malicious program called Stuxnet was introduced into the internal network of the uranium enrichment plant in Natanz (Iran). Experts call it a Zero-Day attack, since the worm used a vulnerability in the Siemens Step7 software to infect the programmable logic controller (PLC) [8]. The virus increased the number of revolutions of the centrifuges. As a result, 1,368 out of 5,000 centrifuges failed. Due to economic sanctions, it would have taken years to restore the centrifuges, which forced Iran to begin negotiations on the

cessation of nuclear weapons production. As a result, the Iranian government shut down its nuclear weapons program and began negotiations to lift economic sanctions [10].

1.4.Ransomware.

In 2017, the so-called WannaCry attack swept across the globe, causing significant financial losses to victims and disrupting critical services (including healthcare) worldwide [1]. According to Clear Insurance, it was among the 10 largest cyberattacks in history [9]. The WannaCry attack was an example of ransomware. When such software is installed on a victim's device, it blocks access to or encrypts files. The subtype of software that encrypts files is called crypto-ransomware. The attacker offers the victim a decryption key in exchange for a certain ransom, which is usually paid in cryptocurrency. The WannaCry attack demanded a ransom of $300 in Bitcoin (a cryptocurrency). The attackers later increased the ransom to $600. Although some victims paid the "ransom," it is still unknown whether their files were restored. The attack also disrupted critical services, including Spanish mobile phone company Telefonica. Hospitals in the UK were also affected: ambulances were diverted, calls were not answered or were delayed, and in some cases, even fatal. 19,000 doctor visits were canceled, and the healthcare sector suffered a total of £92 million in losses. Ultimately, the ransomware affected 230,000 computers in 150 countries, causing $4 billion in damage worldwide. Research by the reputable Symantec company and others has shown that a North Korean group was behind the Lazarus attack.

1.5.Attack on the US Colonial Pipeline.

On May 9, 2021, the US President declared a state of emergency, the reason for which was a large-scale attack on the largest pipeline in the US, the Colonial Pipeline [3]. The pipeline originates in Texas and supplies fuel to the southeastern part of the US. On May 6, 2021, 100 gigabytes of information were stolen from the company. And on May 7, a powerful cyberattack was carried out. The type of attack was a blackmail/ransomware program. According to the Federal Bureau of Investigation (FBI), the hackers demanded 75 bitcoins (4.4 million US dollars), which the company paid [2]. As a result, they received the appropriate means from DarkSide to

restore the system, although this took quite a long time. In addition, the price of a gallon increased by $3.04, which is a historical maximum in the last 7 years. Numerous gas stations were left without fuel in at least 4 states. 87 of the stations in the US capital were empty. People were collecting fuel in various containers from available stations. Flights were delayed from several airports. Panic ensued. [14]

2. Supply chain attacks.

At the end of 2020, the company FireEye released information that an unidentified hacking group had “hacked” the company’s computer system and stolen confidential tools intended for testing the security of information systems [4]. The company, like about 300,000 clients in many countries around the world, uses software from the company SolarWinds to manage computer networks. The hacking group disguised the malware as another update on the SolarWinds update server. Fireeye’s information system automatically updated Solarwinds, as a result of which it was infected [7]. The investigation revealed that more than 18,000 clients worldwide downloaded the malicious Solarwinds update. In the US, the victims of the cyber incident included federal agencies, including the Department of Homeland Security, the Pentagon, the State Department, the Nuclear Nonproliferation Agency, the Treasury Department, the National Institutes of Health, the Department of Energy, and the Department of Finance and Commerce. From the private sector, Microsoft itself became a victim of the cyber incident. The authoritative American publication “The Washington Post”, citing an anonymous source from the investigative bodies, states that the cyber group of the Russian Foreign Intelligence Service APT29, also known as “Cozy Bear”, was behind the operation. The Russian side, traditionally, calls this accusation baseless. [5] The described cyber operation is unique in terms of the selection of the target, planning and flawless execution. The type of cyberattack itself is well known in the field of information security and is called a "Supply Chain Attack."

3. Recent Alarming Cyber Attacks against Critical Services

3.1.Water supply

In February 2021, a hacker infiltrated the control software of the water treatment plant in Oldsmar, Florida and briefly raised the concentration of sodium hydroxide (lye) in the water supply from the normal 100 parts per million to a dangerous 11,100 ppm. The intrusion was made via remote-access software (TeamViewer) on an outdated, poorly secured system — vulnerabilities experts say are common in under-resourced municipal utilities. A plant operator spotted the malicious activity in real time and reverted the change before any contaminated water reached the town, preventing a public-health disaster. Because drinking-water systems are part of a country's critical infrastructure, such cyber-intrusions are not just a criminal matter — they represent a significant threat to public health, economic stability, and national security. Experts have warned the incident should act as a wake-up call: many water and wastewater utilities lack basic cyber-hygiene, proper access controls, or robust operational technology (OT) defenses, making them dangerously exposed.

3.2.Travel

In 2025 a major cyber-attack disrupted operations at several European airports when the software of Collins Aerospace — responsible for check-in and boarding systems at dozens of hubs — was hit by ransomware. As a result, automated check-in, baggage drop and boarding systems went offline at key airports such as Heathrow Airport (London), Brussels Airport and Berlin Brandenburg Airport. Airlines and airport staff reverted to manual check-in and boarding procedures, leading to widespread flight delays, cancellations and long passenger queues. This incident has been widely viewed as a wake-up call about the vulnerability of critical infrastructure in the aviation sector — exposing how dependency on third-party digital systems can create systemic risks for national and international travel.

3.3.Healthcare

In early August 2023, Prospect Medical Holdings — which runs dozens of hospitals and over 150 clinics across multiple U.S. states — suffered a large-scale ransomware attack by the group Rhysida. The attackers reportedly exfiltrated more than 1 TB of data (including a 1.3 TB

SQL database) containing sensitive personal and health-care information belonging to patients, employees and dependents — full names, Social Security numbers, driver's licenses, medical records, diagnoses, lab results, treatment/insurance data, and more. As a result of the breach, many hospitals under the group had to shut down emergency rooms, redirect ambulances, suspend elective surgeries and outpatient services, and revert to using paper records. The company notified affected individuals, offered credit-monitoring and identity-protection services, and launched investigations in cooperation with law-enforcement — but the incident underscored serious vulnerabilities in cybersecurity in the U.S. health-care sector.

4. Discussion

The listed software and non-software tools represent the greatest challenge for the cybersecurity of states, i.e. for national security today. Even the Stuxnet case made several things clear. First of all, after the attack, public awareness of cybersecurity issues increased. Cybersecurity strategies of a number of states were created, changed and updated. According to the report of the Cyber Defense Project "Hotspot Analysis: Stuxnet",

- The state should cooperate with the private sector in the process of protecting critical infrastructure;
- The state should have plans for dealing with cyber attacks such as Stuxnet;
- Countries should have cybersecurity standards for infrastructure assets.

Despite a number of measures, in today's reality, 100% efficiency by states in the fight against cyber threats has not been achieved. It is impossible to completely eliminate technical means, since this reflects the capabilities and signature techniques of hackers; however, depending on the source of the threat, various countries have developed mechanisms that do not completely eliminate, but at least reduce information security risks to some extent.

High awareness is essential. Judging by the cases discussed, criminals often use as a means of attack those people who directly work with information systems. Despite the fact that hundreds of thousands of people are employed in the public sector, agencies should work on raising information security awareness, using training courses, lectures, e-learning platforms, phishing simulations, and other tools. The issue of mandatory training is also important. For some civil servants, information technologies are not of particular interest, which is why they are not interested in security training voluntarily and remain vulnerable to cyber threats. Therefore, it is very important to cover the public sector completely with mandatory retraining programs, especially since threats in cyberspace are increasing every day and the severity of their harmful consequences is also growing. Attracting qualified personnel is another challenge. As in many foreign countries, there is a lack of qualified personnel in the field of information security in our country. One of the reasons for this is the novelty of the field, and another is the difficulty of obtaining academic education. In addition, remuneration in the public sector is less attractive for qualified personnel in this field, since employers in the private sector offer much higher remuneration.

Taking into account cyber threats in the state procurement process is also essential. As discussed above, the so-called Supply Chain Attack represents a complex issue that includes a number of aspects, starting with the legal framework and ending with thorough testing of software and hardware. Most countries' current procurement legislation does not fully take into account cyber threats and cannot completely avoid risks such as the purchase of computer equipment and software from malicious suppliers. To minimize the risks of Supply Chain Attack, it is vital to develop a special procedure for the procurement of cyber technologies as specific goods and services, where the reliability and security of the product become determining factors.

Conclusion

Thus, the examples discussed in the paper have made clear the importance of cybersecurity as a cornerstone of national security. In most cases, a quantitative method is used to assess the scale and severity of a cyberattack, namely the financial losses suffered by the victim (individual, organization, or state) as a result of a specific action. According to cybersecurity experts, by 2025 the damage caused to the global economy by cybercrime will reach 10.5 trillion US dollars per year. This means that every minute cyberattacks will cause 20 million US dollars in damage to the world economy. As a result of the research, the company "Specops Software" has compiled a list of countries ranked by the number of significant cyberattacks based on data from 2006–2020 [13]. A significant cyberattack is considered an attack on a country's government structures or companies, the losses of which are equal to or exceed one million US dollars. It is noteworthy that the USA is not only the leader in this list, but the number of attacks on it significantly exceeds those recorded in other countries. This is despite the fact that the US Cyber Command receives billions of dollars in funding annually and the country ranks first in the world in the GCI (Global Cybersecurity) Index, with a score of 100 out of 100 [6].

The relevance of the issue of developing cyber capabilities is confirmed by the statement of US President Joe Biden in May 2021. Even the leader of such a country openly acknowledged that the country's critical infrastructure cannot be protected to the appropriate degree and that more work is needed to strengthen cyber capabilities. All this is of great concern to any developed or developing country, as it should be emphasized that although the efforts of countries to combat cyber threats are substantial, they are not sufficiently effective. In the modern world, countries must create opportunities for specialists in the field to combat information security risks through cooperation with the public and private sectors, as well as with the rest of the world, and provide support in order to develop new, innovative, technical and non-technical ways to combat cyber threats.

REFERENCES

1. L. Johnson, "WannaCry: Ransomware attacks show strong links to Lazarus group," Broadcom, 2017. [Online]. Available: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b2b00f1b-e553-47df-920d-f79281a80269&tab=librarydocuments
2. Osborne, "Colonial Pipeline ransomware attack: Everything you need to know," *ZDNet*, 2021. [Online]. Available: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
3. Duckett, "Incremental improvements are not enough as Biden signs order boosting US cyber posture," *ZDNet*, 2021. [Online]. Available: https://www.zdnet.com/article/biden-signs-order-boosting-us-cyber-posture-saying-incremental-improvements-are-not-enough/
4. Congressional Research Service, "Cybersecurity: Selected cyberattacks, 2012–2021," Congressional Research Service, 2021. [Online]. Available: https://crsreports.congress.gov/product/pdf/R/R46974
5. E. Sanger, N. Perlroth, and E. Schmitt, "Scope of Russian hacking becomes clear: Multiple US agencies were hit," *The New York Times*, Dec. 14, 2020. [Online]. Available: https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html
6. International Telecommunication Union, "Global Cybersecurity Index 2020," ITU, 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
7. Jibilian and K. Canales, "The US is readying sanctions against Russia over the SolarWinds cyber attack," *Business Insider*, 2020. [Online]. Available: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
8. K. Zetter, "An unprecedented look at Stuxnet, the world's first digital weapon," *WIRED*, Nov. 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
9. L. Carter, "10 biggest cyber attacks in history," Clear Insurance, 2022. [Online]. Available: https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/
10. M. Baezner and P. Robin, "Stuxnet," ResearchGate, 2018. [Online]. Available: https://www.researchgate.net/publication/323199431_Stuxnet
11. RISIDATA, "CIA Trojan causes Siberian gas pipeline explosion," RISIDATA Database. [Online]. Available: https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion
12. RISIDATA, "Baku–Tbilisi–Ceyhan pipeline explosion," RISIDATA Database. [Online]. Available: https://www.risidata.com/Database/Detail/baku-tbilisi-ceyhan-pipeline-explosion
13. Specops Software, "The countries experiencing the most 'significant' cyber-attacks," Specops Software Blog, 2023. [Online]. Available: https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

14. “Colonial Pipeline ransomware attack,” *Wikipedia*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack