

CYBERSECURITY – THE GREAT CHALLENGE FOR THE UNITED STATES FOLLOWING THE WAR IN UKRAINE

Ivan Veleviski

University of Library Studies and Information Technologies

Abstract: *In March 2023, the United States released their National Cybersecurity Strategy (NCS) late. The delay was due to both geopolitical shifts with the war in Ukraine and domestic incidents with the espionage campaign against federal agencies (2020) and the attack on the Colonial Pipeline (2021). The Congress mandated critical sectors to report cyber intrusions to federal agencies, while the Cybersecurity and Infrastructure Security Agency (CISA) launched initiatives to prepare the private sector for potential cyberattacks. According to the Directorate of National Intelligence (ODNI), China, Russia, Iran, and North Korea are the countries from which the majority of cyberattacks on the United States originate. Cyber defense is comprised of four pillars, "Employee awareness; system protection and security; detection using powerful monitoring tools; and preparation by backing up to another system." This article aims to explain some of the Biden administration's cybersecurity policies and their impact on the digital defense space. The article is written using qualitative methods of induction and deduction, i.e. analysis and synthesis. The conclusion emphasizes that the NCS has played a significant role in strengthening and improving the effectiveness of US cyber defense.*

Keywords: *United States; Cybersecurity; National Security Strategy; National Cybersecurity Strategy; Biden Administration*

INTRODUCTION

Shortly before the invasion of Ukraine in 2022, the Biden administration, led by Chris Inglis,¹ finalized the US National Cybersecurity Strategy to be published in 2023. The revelations of a cyber campaign against federal agencies (2020) and several critical infrastructures (the Colonial Pipeline in 2021) have resulted in diplomatic, police and regulatory measures by the government. At the same time, the Cybersecurity and Infrastructure Security Agency (CISA) launched a comprehensive plan to mobilize the private sector in anticipation of cyberattacks by Russia, China, North Korea and Iran. At the end of 2022, fundamental measures were taken to strengthen cybersecurity practices in the federal sector and some critical infrastructure. Several laws aimed at banning the Chinese application TikTok for threatening national security; those were initiated in Congress. The United States National Cybersecurity Strategy of March 2023 is the first official document to specifically address cyberspace issues in the context of cybersecurity. In its 2024 report, CISA noted a 15% increase in cyberattacks compared to the previous year, meaning that the threat remains high. In parallel with this growing threat, CISA points out that "attacks for espionage purposes are the ones that have mobilized operational teams the most." In its report, CISA points to the Pegasus spyware, discovered on the phones of politicians and businessmen. The National Cybersecurity Strategy

(2023) is not an event to be treated in isolation. This document crystallizes decades of debate about the nature of the cyber threat, the referent of cybersecurity, the policy that should be adopted regarding cyberspace resources, and the tools that should be implemented to ensure the security of the USA. As a starting point for the renewal of American power through cybersecurity, the policies developed and implemented since 2021 combine elements of both continuity and disruption.

METHODOLOGICAL APPROACH

Qualitative method for accessing in-depth information; research characterized by flexibility and openness to variables, methods of information collection, synthesis and analysis, induction and deduction.

THE INCIDENT THAT INFLUENCED THE DEVELOPMENT OF THE FEDERAL CYBERSPACE SECTOR

In its report presented on March 11, 2020, the Solarium Commission on Cyberspace considered that the key to cybersecurity is the reform of the organization and structure of the federal government. The Commission was created by the National Defense Authorization Act of 2019 to build consensus on the strategic advantages of the United States in the field of cyber defense. In 2007, under the auspices of President Bush, the National Protection and Programs Directorate (NPPD) was established. Its primary mission was to reduce risks to critical American infrastructure, in the digital domain, after the cyberattack suffered by Estonia in May 2007. However, the department remained marginalized, having failed to attract qualified personnel during the presidency of Barack Obama. The department continued to exist with a deficit of budgetary, political and human resources. The three major incidents of 2014 and 2016-2017 caused a significant change in the mentality of American politicians. In December 2020, a meeting of the US National Security Council was held on massive cyberattacks. It was concluded that data from the US Treasury Department and the Department of Commerce were “monitored”. It was concluded that all US agencies, could potentially be “monitored”, which sent shivers down the spines of American politicians. The question arose as to how mass surveillance of sensitive US data is possible? Experts believe that this stems from the specificity of the cyberattack, such as a “supply chain attack” or “bounce attack”. SolarWinds, a company specializing in high-level IT management and software provisioning for government agencies, was attacked. One of these software programs was hacked and discreetly modified in these IT updates to integrate remote management and surveillance tools. When government agencies using this software updated their software, they could be tracked without anyone noticing. We also need to change the image we have of a Hollywood-style cyberattack. It’s not about software crashes or computers crashing or displaying black screens. “The goal of this type of attack is not to destroy data, but to collect and retrieve it,” emphasizes Loic Guezot.² (Delmas 2020) “So it’s about being as stealthy as possible.” This cyberattack also turned out to be stealthy. For months, the data was recovered without anyone noticing.

Eventually, cybersecurity firm FireEye spotted the problem and, understanding its origins and potential scope, raised the alarm. But an attack of this scale is extremely rare. “It’s almost unprecedented.” The only comparison is perhaps the massive cyberattack on Ukraine in 2017 by the NotPetya virus, which infiltrated ordinary and updated software, which contaminated about thirty banks, ATMs, gas stations and supermarkets. By the way, even automatic radioactivity sensors in Chernobyl failed. In total, 10% of the country’s computers were destroyed, and the cost of this virus is estimated at \$ 10 billion worldwide.

PUBLIC SECTOR

The process of digitalization of the administration has increased the risk of cyberattacks, but other key factors targeting the public sector have also emerged, including: 1. Destabilization of society, such as wars or health crises, is a weapon of choice available to states for political purposes. 2. With the development of more sophisticated online services, they require in-depth knowledge of current data processing regulations, identification of data flows and their security to prevent misuse. 3. The pandemic, which has resulted in a revolution in working methods and a growing reliance on remote working, has forced government agencies to further secure their external communications. 4. The heavy reliance of public administrations on the management and provision of their IT infrastructures by external service providers is also a major factor in their vulnerability to cybersecurity. 5. The Cloud is increasingly establishing itself as a key enabler for the digital transformation of the public sector. This advancement in data and file storage presents an increased risk of cyberattacks. 6. Finally, “Ransomware-as-a-Service” (RaaS) has experiencing rapid success and has particularly been affecting public administrations. By offering hackers, often for a modest subscription fee, a range of comprehensive attack services (tools, a portal to information systems, and even user support and dashboards), RaaS lowers the barriers to entry for cybercriminals.³ (Monty, Dubost, Bouin, Grosseil 2022) Faced with an unprecedented threat, the public sector remains a major target for cyberattacks due to the essential services it provides to our society. However, the sector is gradually moving towards a proactive stance in cybersecurity.

CYBERWARFARE: SHARING INFORMATION

AND RESOURCES BETWEEN THE PUBLIC AND PRIVATE SECTORS

Aware of the dangers of cyberwarfare, public authorities are seeking to implement highly adaptable measures to protect against the challenges faced by various public stakeholders. The first of these configurations is the exploitation of private actors by national security agencies. Edward Snowden’s revelations shed particular light on the NSA’s Prism program. Following the 2008 FISA amendments, the agency used data from several US web companies to collect intelligence as part of its post-9/11 counterterrorism efforts. These measures are part of a strategy to instrumentalize digital infrastructure to create or maintain a global networked intelligence architecture. A very important configuration emerged from the Trump I

administration and has been strengthened since 2021: the creation of collaborative structures and practices between the two sectors. The first step is a reversal of information sharing by national security agencies, especially the NSA and Cybercom. Secondly, the private sector, especially in the area of cybersecurity and threat analysis, has chosen to join this collaboration, especially with the Solar Winds affair. Does it take an incident for people to wake up? Today, everything is going well, we are monitoring our information system to identify indicators of compromise. We have more staff and 24/7 monitoring. We are also raising awareness among our agents because they are the gateway to the attack (via phishing emails), but above all, they are the first barrier.” “It is better to have a ‘little cyber’ in each of the agents than to hire an expert,” adds Jean Larumes, founder of Egerie Software.⁴ The attacks of September 11, 2001, showed that in the IT world, the impact can be significant if one of these organizations is infiltrated through cyberspace, as it opens the door to a combined environment. This is also why computer networks are tightly compartmentalized under the supervision of armies of cybersecurity experts. “Target sectors can range from power plants to food suppliers to the medical world, but also, and no less importantly, network service providers. In a world where every organization increasingly relies on IT resources, cyberwarfare can affect any sector as long as it has an effect on the opposing side that can provide an advantage. Cyberwarfare has become an integral part of hybrid warfare scenarios. According to some studies, the sectors currently most affected by cyberattacks are the medical, technology and telecommunications, financial and energy sectors.

THE CYBER SECURITY COALITION

This includes denial-of-service attacks on government, banking and media websites since February 2022, sabotage software targeting government officials, and attacks on the pharmaceutical supply chain. Today, many sectors have already adopted cyber capabilities to protect their IT infrastructure, but some areas are still lagging behind. This, of course, always depends on the investments they make in cybersecurity, which has become essential for the proper functioning of organizations. “Cyber actors who pose a threat are characterized by their motivation and capabilities.” “The most likely enemies are the great powers fighting for hegemony (Russia and China but also Iran and North Korea). These groups are primarily involved in disinformation and cyber espionage. In the context of the war in Ukraine, groups identified as belonging to Russia are trying to sabotage critical infrastructure such as power plants and steal information that could be useful in conducting military operations.⁵ (Taillat 2024, 176p) But it must also be taken into account that, given the ease of access to information on the Internet today, small groups (especially terrorists or hacktivists) can also exert significant influence by using open and easily accessible knowledge. By definition, cyber actors that pose a threat are characterized by their motivation and capabilities. Great powers will be motivated by long-term dominance and will devote significant resources to it, possibly by using specialized groups to cover their tracks (cyber mercenaries), while cyber Criminals will try to

target vulnerable sectors that can provide them with quick financial gains without remaining discreet. Increasing cyber staff “Overall, cyber staff has increased significantly in recent years across multiple sectors. Various national initiatives are combining efforts aimed at increasing our cyber resilience. CISA is recruiting experts to strengthen its capacity to respond to national crises. The Cyber Security Coalition is undertaking various initiatives to share expertise and connect the worlds of industry, academia and government. The Cyber Security Coalition organizes working groups to exchange knowledge on cybersecurity awareness, as well as other areas of cybersecurity. The Ministry of Defense, for its part, continues to invest in its cyber capabilities, both its own and those intended for civilian and military use. Cyber defense is composed of four pillars: “Awareness among employees; protection and security of the system; detection using powerful monitoring tools; and preparation by making backup copies of another system.

CONCLUSION

1. The publication of the NCS in 2023 crystallizes a decades-long debate on the nature of the cyber threat. The global health crisis has accelerated digitalization, but has also opened up opportunities for cybercrime.

2. Cybersecurity encompasses all means of ensuring the protection and integrity of data, whether sensitive or not, within the digital infrastructure. Cyberattacks include paralyzing systems, stealing sensitive data, blocking access for ransom, forging or damaging documents, and distributing content without the owner’s knowledge.

3. Risks with serious consequences and data loss and financial losses: According to Orange Cyberdefense, cyberattacks increased by 13% in 2023. Small and medium-sized enterprises (SMEs) are most affected, as they are the target of 3 out of 4 attacks. The highest risk remains ransomware (malicious extortion software that takes personal data hostage and demands a ransom payment from the victim to restore access), which represents 38% of the recorded incidents.

4. Devaluing corporate assets: A survey by the CISA agency analyzed 30 major cybersecurity incidents in 28 global companies between 2008 and 2017. Two-thirds of these companies experienced an impact on their stock market value, with a loss of 10%, or even 20%, for the least responsible and least prepared companies.

5. A growing sector with a labor shortage: The cybersecurity field is profitable and growing rapidly, according to a report by Talents du Numérique. The need for qualified and specialized professionals is such that more than 500,000 positions are available in Washington and New York in this sector for all types of degrees and levels of experience.

6. Securing Active Directory and Resilience: While many companies have adopted effective protection technologies such as EDR (Endpoint Detection and Response), a solution for detecting security threats to digital devices, and multi-factor authentication, Active Directory (the nerve center of Microsoft’s information security systems) needs to be better protected, with only 24% of organizations ana-

lyzing incidents in their cyber monitoring center.

7. Optimizing the security of industrial information systems: This is the biggest challenge facing the industrial sector. The firm's study highlights that efforts are being made to deploy a dedicated cybersecurity organization and to use firewalls to separate corporate networks from industrial networks, but more needs to be done.

8. Combating poor cloud security practices: The study highlights security vulnerabilities specific to the cloud. These poor practices include administrative access to a cloud system using a simple login and password. 10. Develop public-private partnerships: The risk of cyberattacks not only affects companies and individuals, but also critical infrastructure, such as power plants and hospitals. Therefore, public-private partnerships aimed at responding to cyber threats and ensuring a secure future for all should be increasingly developed.

9. Cybersecurity policy relies on regaining control and rebuilding cyberspace resources in order to correct its supposed initial trajectory. US control over the global cyberspace architecture has allegedly been too permissive, providing insufficient incentives for operators to place security imperatives at the heart of networks and systems.

NOTES

1. Chris Inglis is a Department of Defense (DOD) and National Security Agency (NSA) veteran, the inaugural Office of National Cyber Director (ONCD) and architect of the United States National Cybersecurity Strategy

2. DELMAS, J.L., 2020. C'est quoi cette histoire de cyberattaque qui a touché le gouvernement?,

Available from: <https://www.20minutes.fr/high-tech/2931807-20201214-etats-unis-quoi-histoire-cyberattaque-touche-gouvernement>

3. MONTY, R. DUBOST, A. BOUIN, A. GROSSEIL, F, 2022. Le secteur public face aux défis de la cybersécurité

Available from: <https://www.groupeonepoint.com/fr/publications/le-secteur-public-face-aux-defis-de-la-cybersecurite/>

4. *Var-Matin*: The online newspaper. Available from: <https://www.varmatin.com/>

5. TAILLAT, S., 2024, 176p. De la Sybersecurite en Amerique, p.176, Paris :PUF, 2024

КИБЕРСИГУРНОСТ – ГОЛЯМОТО ПРЕДИЗВИКАТЕЛСТВО ЗА СЪЕДИНЕНИТЕ ЩАТИ СЛЕД ВОЙНАТА В УКРАИНА

Резюме: През март 2023 г. Съединените щати публикуваха своята Национална стратегия за киберсигурност (NCS) със закъснение. Забавянето се дължи както на геополитически промени с войната в Украйна, така и на вътрешни инциденти с шпионската кампания срещу федералните агенции (2020 г.) и атаката срещу Colonial pipeline (2021 г.). Конгресът е задължил критичните сектори да докладват за кибернахлувания на федералните агенции, докато Агенцията за киберсигурност и сигурност на инфраструктурата (CISA) е стартирала инициативи за подготовка на частния сектор за потенциални кибератаки. Според Дирекцията за национално разузнаване (ODNI) Китай, Русия, Иран и Северна Корея са страните, от които произхождат по-голямата част от кибератаките срещу Съединените щати. Киберзащитата се състои от четири стълба: „Осведоменост на служителите; защита и сигурност на системата; откриване с помощта на мощни инструменти за мониторинг; и подготовка чрез архивиране към друга система“. Тази статия има за цел да обясни някои от политиките за киберсигурност на администрацията на Байдън и тяхното въздействие върху пространството на цифровата отбрана. Статията е написана с помощта на качествени методи на индукция и дедукция, т.е. анализ и синтез. В заключението се подчертава, че NCS е изиграла значителна роля в укрепването и подобряването на ефективността на киберзащитата на САЩ.

Ключови думи: Съединени щати, киберсигурност, Стратегия за национална сигурност, Национална стратегия за киберсигурност, администрация на Байдън

Ivan Velevski, PhD Candidate

Scientific Advisor: Prof. Nano Ruzin, PhD

University of Library Studies and Information Technologies
Sofia, Bulgaria

E-mail: ivovelevski@gmail.com