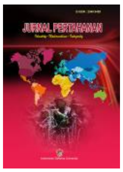

Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 9 No. 3 (2023) pp.542-558
https://jurnal.idu.ac.id/index.php/DefenseJournal

United States National Strategy for Defending Vital Infrastructure from Cyberattacks

Cepi Novia Tristantri[1*], Haryo Prasodjo[2]
[1,2]University of Muhammadiyah Malang, Indonesia

cepinoviatristantri@webmail.umm.ac.id[1*], haryoprasodjo@umm.ac.id[2]
*Corresponding Author

Article Info

Article history:
Received: August 20,, 2023
Revised: December 1, 2023
Accepted: December 24, 2023

Keywords:
Cyber Security,
Cyber Attack,
Data Defense and Security,
National Strategy,
United States of America

DOI:
http://dx.doi.org/10.33172/jp.v9i3.16970

Abstract

The expanding information and communication technology landscape has led to complex security challenges, marked by dynamic and evolving cyber threats including hacking, malware, phishing, data theft, fraud, and Distributed Denial of Service (DDoS). Notably, the United States has faced the highest incidence of cybercrime cases from 2017 to 2021, affecting 2.9 billion victims and resulting in a cumulative material loss of US$18.7 billion during this period. This research centers on the United States, acknowledged as the primary target for global cybercriminals, comprising 38% of cybercrime targets. This research aims to find out the strategic efforts of the United States in overcoming cybercrime that befell its country so that it becomes the best country in cases of alleviating and controlling cases of cyberattacks even though it is also the country with the highest cases of cyberattacks in the world. Utilizing a qualitative research method, the study demonstrates that the United States collaborates systematically and synergistically with state governments, employing a centralized approach to delegate specific tasks and authorities. The study concludes that the United States has implemented the National Cybersecurity Strategy (NCS) 2023 program, aiming to establish a strategic environment and ecosystem by maintaining vital infrastructure and centralized integration.

INTRODUCTION

Technology is used in various fields, such as economics, health, information, business, and education (Alothaim, Hussain, & Al-Hadhrami, 2022). Rapid developments in the field of technology aside from facilitating human life, can become a serious loophole for cybercrime which is worrying (Horowitz, 2020). Cybercrime first received serious world attention in 2011 when a cyberattack occurred on the Iranian nuclear reactor facility, Stuxnet (Harianja, Arianto, & Setiawan, 2022). Szczypiorski (2020) stated that cyberspace and security systems are inseparable units. It is not only a place for exchanging information but also a new place to socialize.

Cyber threats that concern the country's national security have the potential to carry out attacks on the country's strategic projects, such as the security sector, government services, public health, information and telecommunications, transportation, to energy (Tongkachok, Apinawatawornkul, Promsaka, & Sakolnakorn, 2021). Due to the increasing risk of threats to cybersecurity and digital systems, adequate support of facilities and infrastructure is needed (Temple et al., 2023). Along with the development of the digital world, more and more data will be processed automatically (Calix, Singh, Chen, Zhang, & Tu, 2020). This kind of action is then referred to as a cyberattack/cybercrime.

Tenis & Santhosh (2022) understand cybercrime as an act of crime caused by the use of internet technology. Cybercrime is the activity of a person, group of people, or legal entity that uses computers as a means of committing crimes, or makes computers the target of crime (Wahid, 2020). Encyclopedia Britannica defines cybercrime as the use of computers for illegal purposes, such as fraud, trading of child pornographic content, identity theft, and invasion of privacy (Rawindaran, Jayal, & Prakash, 2022). The main difference between cybercrimes and conventional crimes is the presence of technology that facilitates these crimes. According to West Java Regional Revenue Agency (2017) there are several types of cybercrime, such as entering the system illegally, entering content illegally and inappropriately, theft of user data, acts of espionage and sabotage, imitation of other parties' digital products, and disclosure of personal data that is private.

The United States has established a series of policies, laws, standards, and various preventive measures to protect the security of its data and information. Asian countries are far behind when compared to the United States (Kandasamy, Srinivas, Achuthan, & Rangan, 2022). These various efforts were made because cyber security has an important role in the field of information technology. Tatarinova, Shakirov, & Tatarinov (2016) in their research said that an important task facing the government, especially law enforcement officials and scientists in the rapid development of information technology, is to prevent crimes from being committed and find the best way to deal with cybercrime problems (Dasril, 2020).

Based on a report compiled by the United States cybersecurity service company, Surfshark, there were 43.19 million accounts in the world that experienced data leaks in the first quarter of 2023. From 2004 to 2022, the United States experienced nearly 2,000 cybercrimes in the form of data theft of 5 billion accounts making it the country with the largest personal data theft cases in the world (Surfshar, 2023). Verizon's report on Data Breach Investigations Report (DBIR) states that the entertainment industry is the industry that most frequently experiences data leaks in 2021 with a total of 7,065 cases out of a total of 29,207 incidents throughout 2021 (Burbidge, 2021). The Yahoo data leak case in August 2013 is the largest data leak case in current history. Yahoo said that there were around 3 billion accounts on their leaked service (Hill & Swinhoe, 2022).

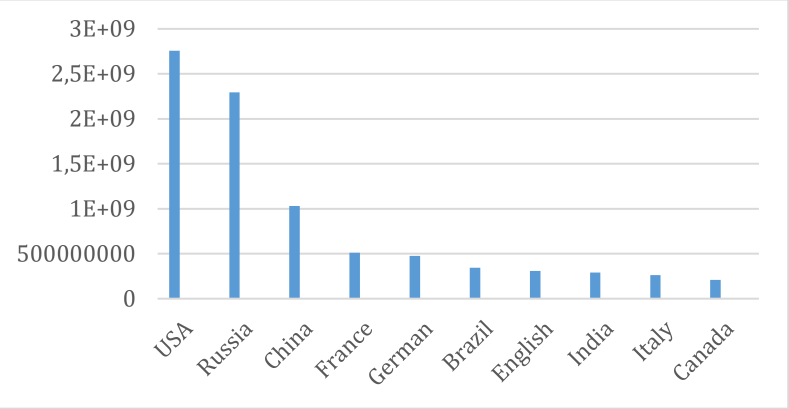

Figure 1. 10 Countries with Highest Data Theft in 2020-2022 (Surfshark, 2023)

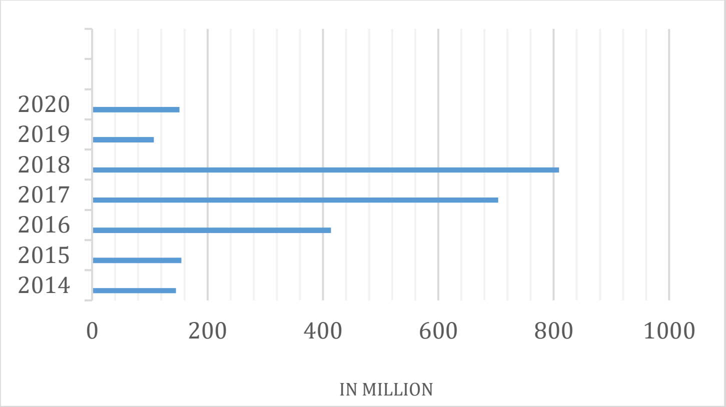

Figure 2. Number of Data Theft Victims in the World's Largest Cases in 2014-2020 (Purple Security, 2023)

Figure 1 shows that the United States is the country with the highest cases of data theft from 2020-2022 with a total of 2.8 billion victims. Followed by Russia ranked 2nd with 2.3 billion victims. From Figure 2, it can be seen that the number of victims of cyber-attacks has a positive trend with a gradual increase from 2014 which reached around 150 million victims until it experienced its highest peak in 2018 with a total of around 820 million accounts/users. However, cyberattacks decreased drastically in 2019 with only 110 million accounts, and increased again in 2020 to around 150 million accounts. One of the driving factors for the decline in cybercrime in 2019 was the incessant passage of laws and cooperation between sectors in various countries (Amin & Huda, 2021). Such as the cooperation between the United States and Indonesia in the form of cyber security investments (Judith, 2019), the cooperation between the United States and ASEAN countries through the 2019 Indo-Pacific strategy program United States Department of State Office of the Spokesperson, 2019 as well as the United States bilateral cooperation with China by using the concept of cybersecurity.

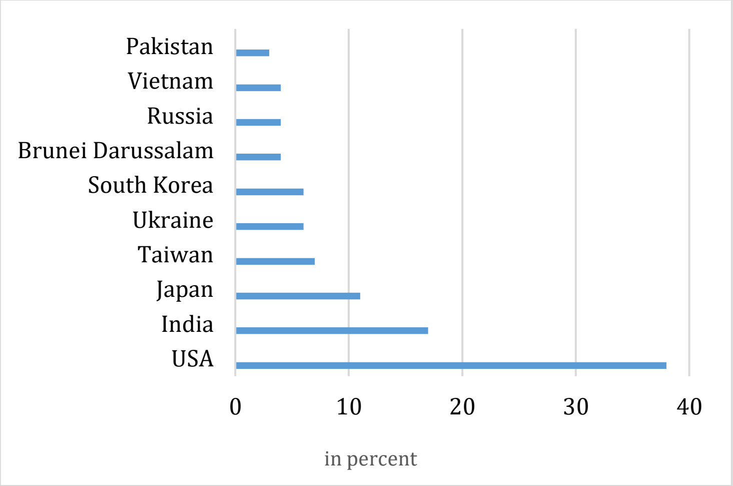

Figure 3. Percentage of Countries as Cyber Attack Targets in 2022 (Purple Security, 2023)

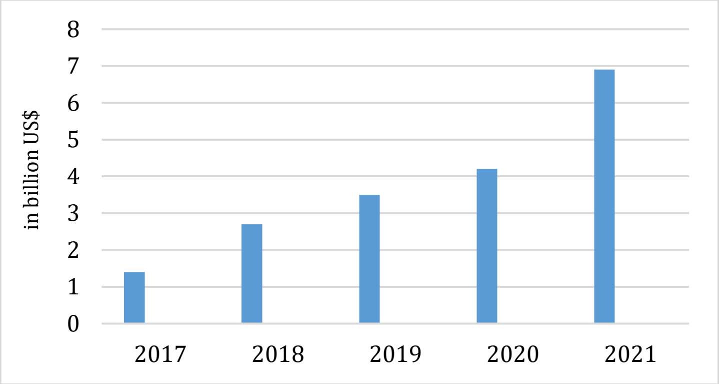

Figure 4. World Cyber Crime Losses Report 2017-2021 (Federal Bureau of Investigation, 2022)

Figure 3 shows the percentage of countries in the world as the highest cybercrime destination in 2022. The United States occupies the top position with a percentage reaching 38%, then India reaching 17%, and Japan with 12%. Cybercrime causes material losses that are not insignificant. From Figure 4, it can be seen that there has been a significant increase in material losses in the world from 2017 to 2021. In 2017 the world's material losses from cybercrime reached US$1.4 billion, which increased in 2018 to US$2.8 billion, to reach its highest peak of increase in 2021 with a total loss of US$6.9 billion. Losses due to cybercrime reached their highest peak in 2021 due to the COVID-19 pandemic with the existence of lockdown regulations, work from home (WFH), and the high death toll due to COVID-19-19, so this weakened the security of both personal and organizational data (CNN Indonesia, 2023).

The data presented in Table 1 shows that the total material losses caused by cybercrimes continue to increase from year to year. Initially, in 2017 the United States suffered a loss of US$1.4 billion in 2018, 2019, and 2020 respectively to US$2.7 billion, US$3.5 billion, and US$4.2 billion and achieve the highest loss in 2021 it will reach US$6.9 billion. 2021 will be a year with a significant increase in material losses by a difference of US$2.7 billion compared to 2020.

Table 1. Data on Cyber Crime and Cyber Loss Reports in the United States for 2017-2021 (Federal Bureau of Investigation, 2022)

Year	Total Report		Total Loss (billion US$)
2017	301,580		1.4
2018	351,937		2.7
2019	467,361		3.5
2020	791,790		4.2
2021	847,376		6.9
Total:	2,72 million reports	US$18,7 billion	

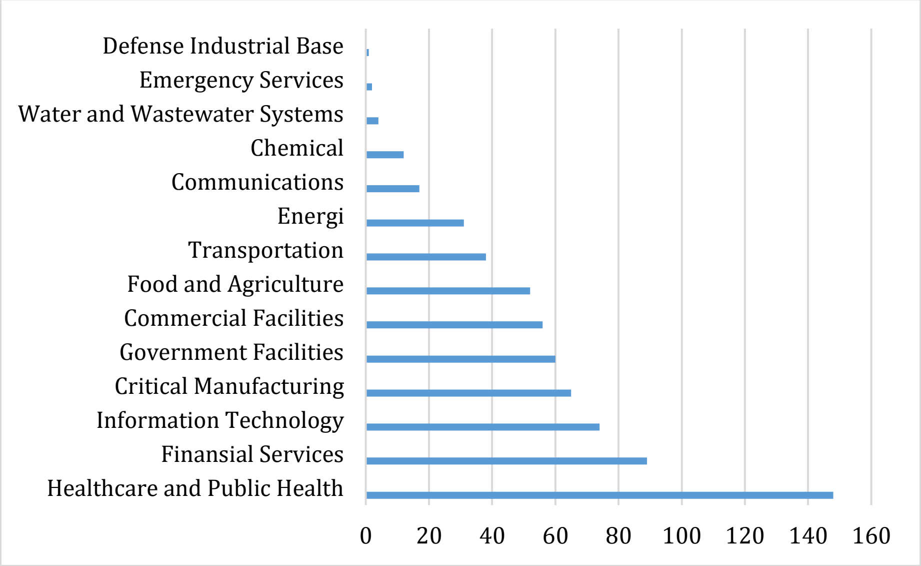

Figure 5. Cyber Ransomware Attacks on 14 Infrastructure Sectors in the United States in 2017-2021 (Federal Bureau of Investigation, 2022)

With so many losses caused by cybercrime in the United States, of course, the public service sector is also a target for crime. Figure 5 is a list of public infrastructure sectors that have been targeted by cybercrimes in the United States in the 2017-2021 period. Health and public health services are the sectors with the highest incidents of cybercrime in the United States with a total of 150 cases/incidents of cybercrime. The second sector is financial services with 90 cases, and the defense industry sector has only one case of cyberattacks in the last five years.

Based on the data above, it can be concluded that cyber security is an important matter and has a high urgency considering the impact it has is so large and touches vital and strategic aspects of the state as well as individuals. Cases of cybercrime in the United States in the form of hacking and theft of personal data are very worrying because they threaten the security and safety of the people, institutions, and even the very existence of the state. Cybercrime cases are not only a country's problem, but all countries in the world because it also has the potential to cause conflict between countries.

This research aims to find out the strategic efforts of the United States in overcoming cybercrimes that befell its country so that it becomes the best country in cases of alleviating and controlling cases of cyberattacks even though it is also the country with the highest cases of cyberattacks in the world. It is hoped that the strategy adopted by the United States can inspire other countries to overcome this problem. Cyberattacks occur all over the world from continent America, Europe, and Australia, to Asia. So that this research is needed as learning material and additional reference for students, lecturers, and the public to enrich insight and make it a reference in handling cybercrime cases in other countries by adopting and adapting strategies for handling cybercrime implemented in the United States.

METHODS

The research method used in this study is qualitative. The samples used are references from books, journal articles, and official websites of reputable agencies and news media, such as VOA, CNN Indonesia, CNBC, and Kompas. Books and journal articles were sourced from Scopus with the search keywords "Cyber Security", "United States Cyber Security", and "United States Cyber Attack". This was then continued by reducing several journal articles that were deemed not appropriate to authorship requirements and obtaining 873 documents in the form of books and journal articles that were relevant to the topic. After that, the Research Information System (RIS) file is downloaded and exported to the Mendeley application to double-check the relevance of the journal articles obtained on the topic. Because the method used is descriptive qualitative, this study focuses on mapping the results of previous findings discussing United States cyber security using the Mendeley application. Apart from that, to support the credibility of the statement, quantitative data is included which comes from the official website of the United States cyber security agencies, such as the U.S. Department of Defense and National Security Agency.

Thus, a qualitative research method was chosen in this study because it was considered the most suitable for research needs when viewed from the topic and formulation of the problem and research objectives which required a lot of literature from previous research from experts as well as data originating from other credible institutions/organizations by field. By using qualitative methods, it is hoped that this research can describe in-depth and comprehensively the phenomenon (Creswell & Poth, 2017) of cybercrime in the United States and describe the strategic efforts made by the United States in preventing and overcoming cybercrime cases as the country with the highest cybercrime cases in the world.

However, the United States is also the country with the best alleviation of cybercrime cases in the world, so it is interesting to discuss further to be able to know, understand, and adopt the values and various strategies undertaken by the United States in suppressing cybercrime cases in their country. Either by establishing national policies/laws, creating cyber monitoring institutions, or establishing strict cyber/cyber standards. It is hoped that the strategy adopted by the United States can inspire other countries to overcome this problem.

RESULT AND DISCUSSION

United States President Joe Biden's Directive on Forming a National Strategy to Address Cybercrime in the United States

Joe Biden on March 1, 2023, then gave a press statement about increasing cyber security in the United States. Biden said that cybersecurity is vital in safeguarding the economy and all strategic infrastructure, democratic institutions and systems, information and telecommunications, privacy, and the United States' defense sector (Widakuswara, 2023). Biden appointed a senior White House cybersecurity official to plan and execute an Executive Order to improve cybersecurity in the United States and build positive collaborations with the public and private sectors. In general, the issuance of an Executive Order later aims to protect data on United States citizens from cybercriminals, hold them formally accountable for any acts of cybercrime committed, as well as defend against any cyberattacks that threaten the data and privacy of United States citizens (Benjamin, Zhang, Nunamaker, & Chen, 2016).

This order was also carried out by carrying out various collaborations both with actors inside and outside the United States, such as with its allies. This was strengthened internally by socializing the program to industry, civil society, governments in various states, local governments, to several tribes in the United States. This is based on the high number of cases and threats of cybercrime in the United States coupled with the rapid development of the digital world. The efforts/strategies contained in the Executive Order will also seek to guarantee open, global, safe-to-use, and high-speed internet access that can be relied upon by the citizens of the United States.

United States National Cybersecurity Strategy (NCS) 2023

This strategy is built on significant achievements in cyber security defense to be able to form a strategic environment and ecosystem (US Strategic Command, 2023). United States President, Joe Biden named a senior White House leader in cybersecurity to new positions on the National Security Council (NSC) and Office of the National Cyber Director (ONCD). Programs that contain various strategic efforts of the United States covering the entire territory of the state are listed in the official White House document which consists of five main pillars, namely Pillar I defending vital infrastructure, Pillar II interrupting and avoiding threatening actors, Pillar III establishes market forces to promote cyber security and resilience, Pillar IV by investing in the future, and Pillar V by forging international partnerships in achieving common goals. Furthermore, the author will focus on Pillar I regarding the efforts of the United States to maintain its vital infrastructure (Widakuswara, 2023).

The five-pillar approach creates a comprehensive framework for addressing cybercrime. Pillar one is carried out by prioritizing the security and resilience of critical infrastructure which is a crucial first step. By encouraging collaboration between the public and private sectors, as well as establishing regulations that support best cybersecurity practices, this pillar aims to make cyberattacks more difficult for malicious actors to carry out. The second pillar emphasizes the use of all instruments of national power to disrupt and dismantle threat actors. Involves diplomacy, finance, military, and law enforcement. The third pillar pushing the market towards security and resilience, this pillar focuses on increasing responsibility within the digital ecosystem. Through regulations, incentives, and the establishment of laws governing responsibility and accountability, this pillar aims to address the investment gap in cybersecurity and stimulate the adoption of best practices across the industry. The fourth pillar is to fill investment gaps, especially when building the next digital infrastructure and facing technological revolutions such as artificial intelligence and quantum computing. And pillar five by collaborating with the international community, this pillar creates a broad coalition to safeguard Internet freedom, face common threats, and promote norms of responsibility in state behavior in cyberspace.

The First Pillar, which focuses on the defense of vital infrastructure, is considered more important because critical infrastructure is the foundation of national security and economic prosperity. Attacks on vital infrastructure can have far-reaching and serious impacts on countries, including potential risks to human life, economic stability, and the functioning of society. Some important sectors and services rely heavily on critical infrastructure, such as energy, water, transportation, and communications. The sustainability and operational security of this infrastructure is very necessary to maintain social and economic stability. Attacks on critical infrastructure can have a significant impact on national and international supply chains. If this infrastructure is threatened or disrupted, it can trigger a domino effect that is detrimental to various economic sectors, from production to distribution.

Maintaining Vital Infrastructure

The research places a significant emphasis on the strategic efforts employed by the United States to combat cybercrime, particularly in the context of maintaining vital infrastructure. This is a critical aspect of cybersecurity, as vital infrastructure encompasses sectors crucial for national security, public safety, and economic prosperity (National Security Agency). One noteworthy strategy implemented by the United States is the establishment of the National Cybersecurity Strategy (Widakuswara, 2023). This program aims to form a strategic environment and ecosystem by maintaining vital infrastructure through a centralized integration approach. The Federal Government plays a pivotal role in coordinating the authority and capabilities of various departments and agencies responsible for supporting the defense of vital infrastructure (U.S. Department of Defense). This includes sectors such as healthcare, financial services, information and technology, government facilities, agriculture, transportation, energy, emergency services, and the defense industry.

The Federal Cyber Security Center serves as a collaborative hub, bringing together capabilities across homeland defense, law enforcement, intelligence, diplomatic, economic, and military domains. This centralized integration enables intergovernmental coordination and empowers the Federal Government to effectively and decisively support non-Federal partners. The importance of maintaining vital infrastructure is underscored by the collaboration between the Federal Government and state governments. States have the authority to establish their cybersecurity agencies, contributing to the overall cybersecurity posture. However, this collaboration requires reports and approvals with federal oversight, ensuring a cohesive and synchronized approach to cybersecurity. The division of tasks between the state government and the United States federal government is grounded in principles of federalism, recognizing the shared responsibility for cybersecurity. State governments, equipped with agencies or departments focusing on cybersecurity, collaborate with the federal government on information sharing, training, and coordinating responses to cyber threats. This collaboration is vital due to the cross-border nature of cyber threats, enabling better information exchange, more effective prevention efforts, and faster responses to incidents.

Maintaining systems and assets is vital to the national security, public safety, and economic prosperity of the United States. Collaboration is needed to deal with increasingly varied and sophisticated cyber threats, alleviation of this problem will only be effective if the relevant actors have qualified cybersecurity protection to make it difficult for cybercriminals to carry out administrative hacks (Creemers, 2022). The private sector is needed as a partner to collaborate with the government sector and the public sector to maximize this effort. The private sector has also shown a positive commitment to engage in active and cooperative cyber defense efforts.

Federal States Cybersecurity Centralized Integration

The Federal Government coordinates the authority and capabilities of departments and agencies that are collectively responsible for supporting the defense of vital infrastructure, namely healthcare, financial services, information and technology, government facilities, agriculture, transportation, energy, emergency services, and the defense industry (Federal Bureau of Investigation, 2022). The Federal Cyber Security Center serves as a collaborative node that brings together government-wide capabilities across homeland defense, law enforcement, intelligence, diplomatic, economic, and military. Once fully integrated, they will promote intergovernmental coordination and enable the Federal Government to effectively and decisively support non-Federal partners.

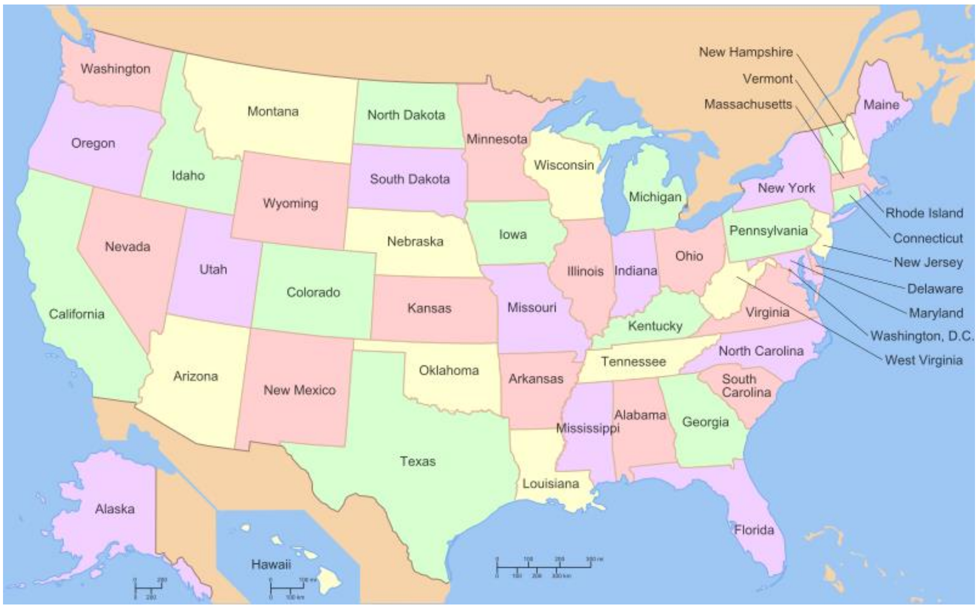

Figure 6. Map of the United States of America (United States Census Bureau, 2023)

Figure 6 shows the distribution map of the 50 states of the United States stretching from Washington to Florida. Out of these 50 states, four of them declare as a commonwealth. Initially, the United States only had 13 states at the time of the Proclamation of Independence on July 4, 1776. This number has continued to grow to date. The state with the highest population is California, which will reach 39 million in 2021 (United States Census Bureau, 2023). Meanwhile, the state with the least population is Wyoming with 515 thousand inhabitants (United States Census Bureau, 2023). Each state is a sovereign entity of its own, so states have the authority to regulate their government as long as it is within the limits set by the United States Constitution. Therefore, state governments vary and no state government is the same as another. From this description, we can conclude that the United States is the largest country in the world in terms of area and population.

However, this condition also poses a serious threat to the United States in ensuring the security and safety of the country and its people, including threats from cybercrimes/attacks.

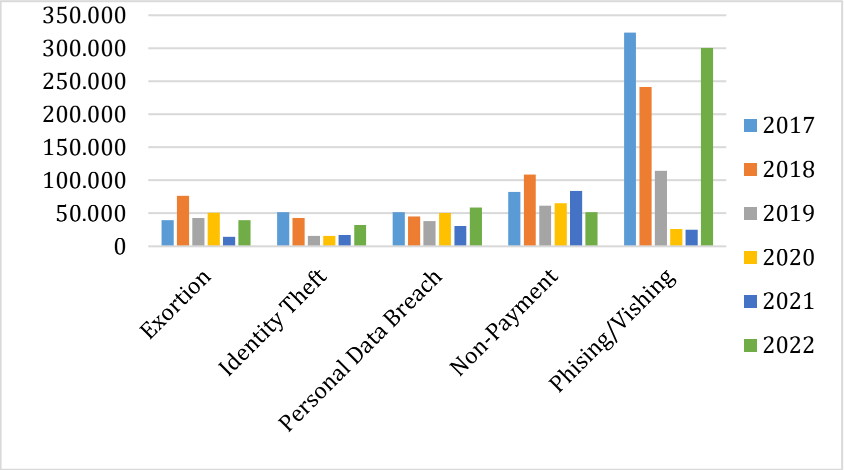

Figure 7. The Five Highest Types of Cyber Crime in the United States in 2017-2022 (Federal Bureau of Investigation, 2022)

During the period 2017 to 2022, the United States witnessed a significant increase in various types of cybercrime affecting various aspects of life. Online extortion crimes have fluctuated over the past five years. The highest peak occurred in 2018 with 76,741 cases, while in 2020 there was a drastic decline to 14,938 cases. Identity theft crimes continue to be a serious concern. The highest peak was reached in 2017 with 51,629 cases, and despite the decline, the number of cases remains significant until 2022 with 32,538 cases. Personal data breaches reached their highest peak in 2022 with 58,859 cases. These crimes involve unauthorized access or disclosure of an individual's personal information, such as identification numbers, financial information, or other personal details, which may threaten an individual's privacy and security. Non-payment crimes involve unauthorized or manipulative payment transactions. In 2018, the number of cases peaked at 108,869 cases, indicating a high level of online financial fraud activity during that period. Phishing/vishing crimes include hacking attempts through online or telephone tricks and manipulation. In 2017, there was a significant spike with 323,972 cases, and despite fluctuations, the crime rate remains high until 2022 with 300,497 cases. This type of fraud is generally aimed at obtaining sensitive information from victims, such as passwords or financial information.

Administration Agencies have made progress in establishing the Joint Cyber Defense Collaboration (JCDC) at CISA to integrate cyber defense planning and operations across the Federal Government and with the private sector and international partners; strengthening the capacity of the National Cyber Investigative Joint Task Force (NCIJTF) to coordinate law enforcement. When Federal assistance is required, the Federal Government must provide an integrated, coordinated, and comprehensive government response. Organizations that are targeted by cyber threats must know which government agencies to contact and for what purposes.

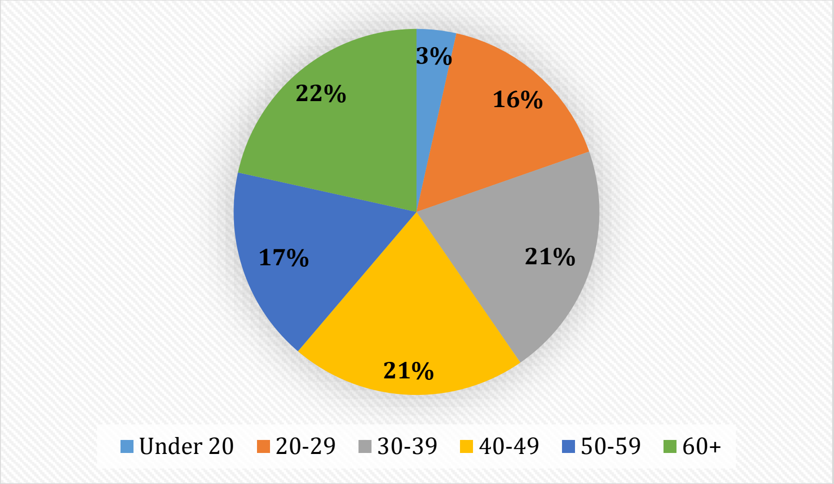

Figure 8. Age Group Percentage of Cybercrime Victims in the United States in 2021 (Federal Bureau of Investigation, 2022)

From the cyberattack data above, the age group of 60 years and over is the group with the highest number of cybercrime victims with a percentage of 22%. It can be understood that the cognitive abilities of the age group over 60 years and over are decreasing, making them vulnerable to becoming targets of cybercrime. The 30-49-year-old group is in second place with a percentage that is not far behind, namely 21%. This age group is a productive age group with high mobility in their daily lives, so it is assumed that they lack attention to cyber security and defense, including data security.

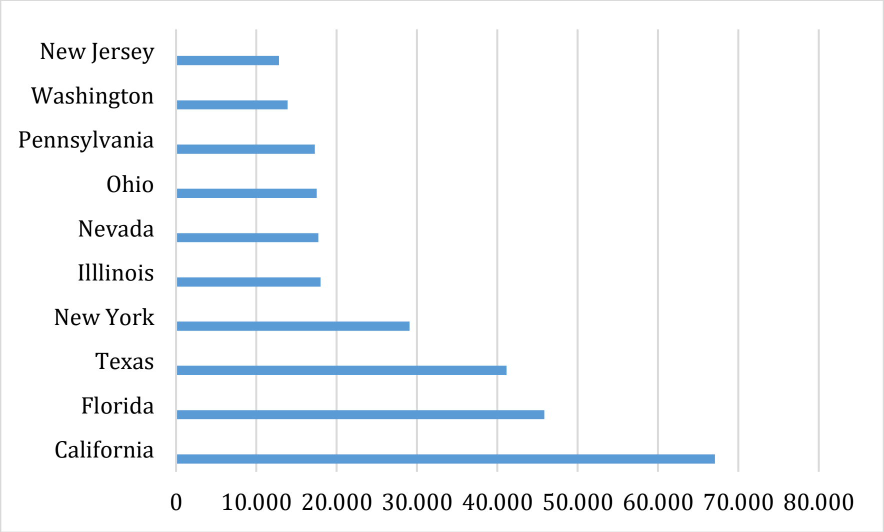

Figure 9. The 10 Largest States in the United States as Victims of Cyber Crime in 2021 (Federal Bureau of Investigation, 2022)

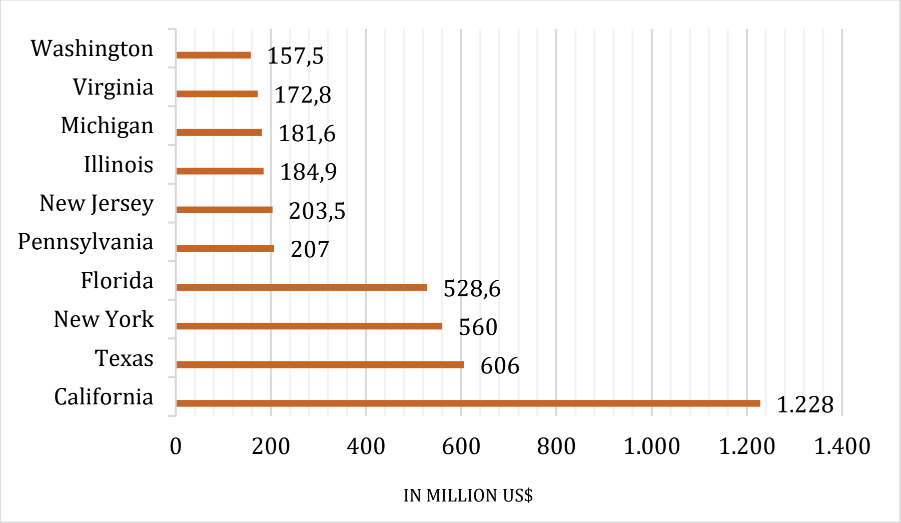

Figure 10. 10 Largest United States' States with the Largest Total Losses due to Cyber Crime in 2021 (Federal Bureau of Investigation, 2022)

From Figure 9, it can be concluded that every state in the United States has the potential to become a target of cybercrime. California became the state with the most cybercrime victims in the United States in 2021 with a total of 68,000 people. Then the states of Florida and Texas respectively amounted to 47,000 people and 41,000 people. New Jersey became the state with the fewest cybercrimes in 2021 with a total of 12,000 users. In line with these data, in Figure 10, a graph of the total material losses arising from cybercrime/attacks that hit federal states in the United States is presented. In 2021, the state of California occupies the highest position with a total loss of US$1.228 million, followed by Texas with US$606 million and New York with US$560 million. From the graphs above, it can be understood that cybercrime is a serious problem that must be resolved immediately because it has a significant impact on material and non-material losses for the existence of the state and the United States itself (Britannica).

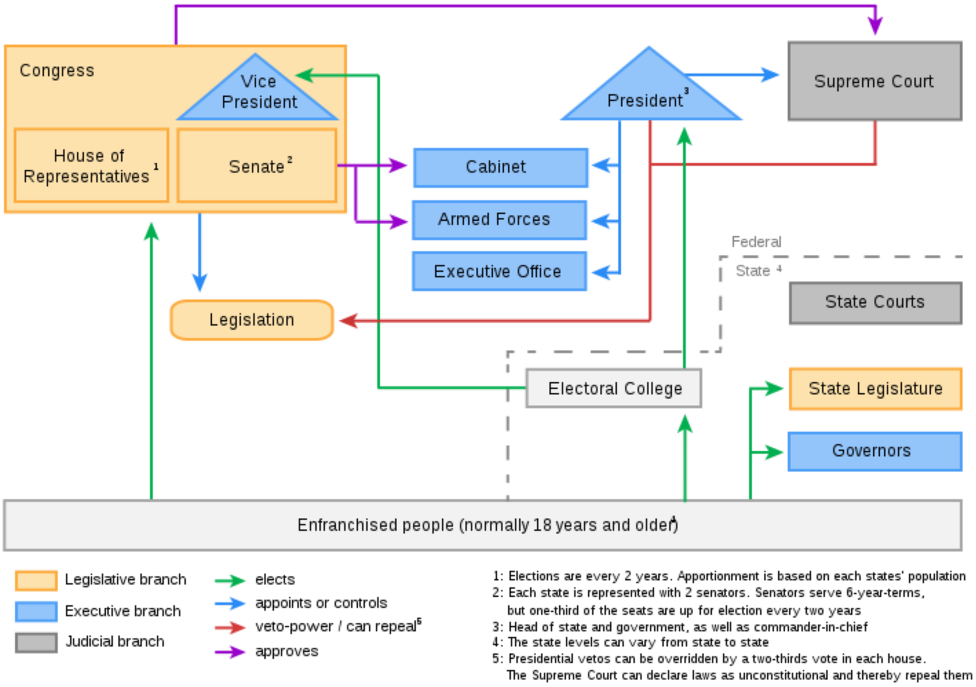
Congress
Vice President
House of Representatives 1
Senate 2
President 3
Supreme Court
Cabinet
Armed Forces
Executive Office
Federal
State 4
State Courts
Legislation
Electoral College
State Legislature
Governors
Enfranchised people (normally 18 years and older)4
Legislative branch
Executive branch
Judicial branch
elects
appoints or controls
veto-power / can repeal5
approves
1: Elections are every 2 years. Apportionment is based on each states' population
2: Each state is represented with 2 senators. Senators serve 6-year-terms, but one-third of the seats are up for election every two years
3: Head of state and government, as well as commander-in-chief
4: The state levels can vary from state to state
5: Presidential vetos can be overridden by a two-thirds vote in each house. The Supreme Court can declare laws as unconstitutional and thereby repeal them

Figure 11. United States Political System (Charles, 2023)

The division of tasks between the state government and the United States federal government in terms of cybersecurity is based on the principles of federalism that govern the relationship between the federal government and state governments. Because cybersecurity has a broad impact and involves many aspects, including national security, personal data, vital infrastructure, and so on, collaboration between the federal and state governments is vital. State governments also have a role to play in cybersecurity, especially in protecting the infrastructure and data in their area. State governments often have an agency or department that focuses on cybersecurity at the state level. State governments can collaborate with the federal government on sharing information, training, and coordinating responses to cyber threats.

Cooperation and coordination between the federal and state governments is vital in dealing with increasingly complex and evolving cyber threats. Due to the cross-border nature of cyber threats, this collaboration enables better information exchange, more effective prevention efforts, and faster response to cybersecurity incidents. The Federal Government needs to provide clear guidance on how private sector partners can contact Federal agencies for support during cyberattacks and what forms of support the Federal Government can provide. Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities (The White House, 2016). In this case, the role of the Cyber Threat Intelligence Integration Center (CTIIC) is needed to coordinate intelligence collection, analysis, and partnerships (Yuvaraj & Venkatanarayanan 2019). Operational collaboration models in Sector Risk Management Agency (SRMA), such as the Department of Energy's (DOE) Center for Energy Threat Analysis (ETAC) pilot, DoD's Defense Industrial Base Collaborative Information Sharing Environment (DCISE), and Central National Security Agency (NSA) Cybersecurity Collaboration provide opportunities to enable information sharing. that are timely, actionable, and directly relevant to private sector partners in their respective sectors.

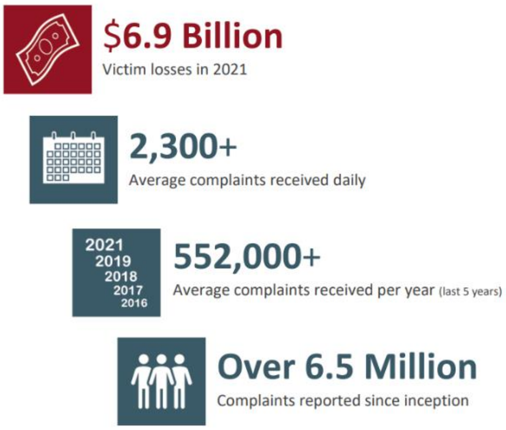

Figure 12. Statistics between Cybercrime Victims and Total Losses Resulted in the United States in 2021 (Federal Bureau of Investigation, 2022)

Further efforts are needed to strengthen and integrate the operational capabilities of the Federal Government and enhance the integration of the Federal Cyber Security Center. ONCD will lead the Administration's efforts to improve the integration of centers like these, identify gaps in capabilities, and develop implementation plans to enable collaboration on cybercrime efforts in the United States.

Combining collaboration between organizations and other technology-enabled actors creates connections that drive collective and synchronized action to protect vital infrastructure. Certification Exam to Certify in IT Audit and Advance (CISA) is the national coordinator whose job is to ensure the security and resilience of the United States' vital infrastructure. In this role, CISA coordinates with the Sector Risk Management Agency (SRMA) to enable the Federal Government to improve its coordination with owners and operators of vital infrastructure across all states of the United States. This SRMA is responsible for increasing security and resilience in the sector and protecting the systems and assets it operates.

United States Strategic Pillars and Imperatives for Improving the Cybersecurity Landscape in 2023

Based on the discussion above, it can be concluded that the United States has taken several significant steps to combat cybercrimes. These include the issuance of President Biden's directive, which emphasizes the protection of vital infrastructure in healthcare, financial services, information and technology, government facilities, agriculture, transportation, energy, emergency services, and the defense industry. Additionally, the creation of the National Cyberattack Strategy (NCS) 2023 and fostering collaboration between the federal and state governments are crucial components of the US approach. From these US initiatives, at least four critical points can be identified as essential for success in dealing with cybercrimes: 1) a country needs a serious political will from its leaders. Without awareness and commitment from leaders, there will be no regulations or concrete actions to effectively address cybercrime; 2) implementing comprehensive cybersecurity measures across critical sectors such as healthcare, finance, and technology is crucial. This involves a combination of defensive and offensive capabilities to deter and respond to cyber threats effectively; 3) a country needs specific regulations or strategic documents outlining how to deal with cybercrimes. These regulations should encompass various aspects, including prevention, response, and collaboration between public and private sectors; 4) the regulations should ensure alignment between the central government and local/regional authorities. Effective coordination and collaboration are essential to creating a unified and coordinated approach to combat cybercrimes at all levels of governance.

The NCS 2023 outlines five pillars, including defending vital infrastructure, interrupting and deterring threatening actors, promoting market forces for cybersecurity, investing in the future, and forging international partnerships. This involves developing measures to deter malicious actors and establishing effective response mechanisms, utilizing both offensive and defensive cyber capabilities. Diplomatic efforts focus on fostering international cooperation, establishing norms of responsible state behavior, sharing threat intelligence, and addressing global cyber threats. Collaboration between government agencies and the private sector is promoted to share threat information, and best practices, and coordinate responses, recognizing the crucial role of private entities. Investments in cybersecurity research and development aim to stay ahead of emerging threats, promote innovation, and enhance overall cybersecurity. There's a focus on developing a skilled cybersecurity workforce through education, training, and recruitment efforts.

CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

The United States faces escalating cyber threats with potential national security implications, impacting critical sectors. Despite experiencing a significant increase in cybercrime and data breaches, the United States has implemented policies and preventive measures. President Biden's directive, the National Cyberattack Strategy (NCS) 2023, and collaborative efforts between federal and state governments underscore a multifaceted approach. Essential elements for success include political will, comprehensive cybersecurity measures, specific regulations, and alignment between central and local authorities. The NCS 2023's five pillars focus on defending infrastructure, deterring threats, promoting market forces, investing in the future, and forging international partnerships. While future research should delve into specific strategies and international perspectives, this study's limitations, including a restricted reference scope and a general overview, emphasize the need for more varied and in-depth investigations beyond Scopus journal articles. Up-to-date and practical implementations, involving diverse stakeholders, can contribute to a nuanced understanding of US cybersecurity strategies and their broader implications.

REFERENCES

Alothaim, A., Hussain, S., & Al-Hadhrami, S. (2022). Analysis of Cybersecurities within Industrial Control Systems using Interval-Valued Complex Spherical Fuzzy Information. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/3304333

Amin, M. E., & Huda, M. K. (2021). Harmonization of Cyber Crime laws with the Constitutional Law in Indonesia. *International Journal of Cyber Criminology*, *15*(1), 79–94. https://cybercrimejournal.com/pdf/ijcc-6-2021.pdf

Benjamin, V., Zhang, B., Nunamaker, J. F., & Chen, H. (2016). Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities. *Journal of Management Information Systems*, *33*(2), 482–510. https://doi.org/10.1080/07421222.2016.1205918

Burbidge, T. (2021). Cybercrime Thrives during Pandemic: Verizon 2021 Data Breach Investigations Report. Retrieved August 3, 2023, from Verizon website: https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

Calix, R. A., Singh, S. B., Chen, T., Zhang, D., & Tu, M. (2020). Cyber Security Tool Kit (Cybersectk): a Python Library for Machine Learning and Cyber Security. *Information (Switzerland)*, *11*(2). https://doi.org/10.3390/info11020100

Charles, G. (2023). *Election Law in the American Political System* (3rd Edition). Los Angels: Aspen Publishing.

CNN Indonesia. (2023). FBI: Kejahatan Siber Meningkat 300 Persen Kala Pandemi Corona. Retrieved August 3, 2023, from CNN Indoensia website: https://www.cnnindonesia.com/teknologi/20200420185452-185-495401/fbi-kejahatan-siber-meningkat-300-persen-kala-pandemi-corona

Creemers, R. (2022). China's Emerging Data Protection Framework. *Journal of Cybersecurity*, *8*(1), 1–12. https://doi.org/10.1093/cybsec/tyac011

Creswell, J. W., & Poth, C. N. (2017). *Qualitative Inquiry and Research Design and Mixed Methods*

Research. New York: Sage Publication, Inc.

Dasril. (2020). *Pengantar Teknologi Informasi*. Solok: CV Intan Cendekia.

Federal Bureau of Investigation. (2022). Internet Crime Report. Retrieved from https://www.ic3.gov/media/pdf/annualreport/2021_ic3report.pdf accessed on October 31, 2023.

Harianja, A., Arianto, A. R., & Setiawan, M. C. A. (2022). Implikasi Perang Siber antara Israel, Amerika Serikat dan Iran melalui Olimpic Game Operation terhadap Fasilitas Program Nuklir Iran pada Periode Pemerintahan Mahmoud Ahmadinejad: Perang Siber Stuxnet 2010. *Moestopo Journal Of International Relation*, *2*(2), 91–117. Retrieved from https://journal.moestopo.ac.id/index.php/mjir/article/view/1895/1094

Hill, M., & Swinhoe. (2022). The 15 Biggest Data Breaches of the 21st Century. Retrieved from: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html accessed on October 31, 2023

Horowitz, B. M. (2020). Cyberattack-Resilient Cyberphysical Systems. *IEEE Security and Privacy*, *18*(1), 55–60. https://doi.org/10.1109/MSEC.2019.2947123

Justiari, M. P. J. (2019). AS Minati Investasi Keamanan Siber, Indonesia Masih Menimbang-nimbang. Retrieved August 16, 2023, from: https://www.kompas.id/baca/utama/2019/11/21/as-berminat-investasi-di-keamanan-siber-indonesia-masih-garap-aturan

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Healthcare-Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access*, *10*, 12345–12364. https://doi.org/10.1109/access.2022.3145372

Purple Security. (2023). 2023 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends for 2023. Retrieved August 4, 2023, from Purple Security website: https://purplesec.us/resources/cyber-security-statistics/#Ransomware

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. *Computers*, *11*(12). https://doi.org/10.3390/computers11120174

Surfshark. (2023). Data breach monitoring. Retrieved August 3, 2023, from https://surfshark.com/research/data-breach-monitoring

Szczypiorski, K. (2020). Cyber(in)Security. *International Journal of Electronics and Telecommunications*, *66*(1), 243–248. https://doi.org/10.24425/ijet.2020.131870

Tatarinova, L. F., Shakirov, K. N., & Tatarinov, D. V. (2016). Criminological Analysis of Determinants of Cybercrime Technologies. *Mathematics Education*, *11*(5), 1127–1134. Retrieved from https://www.iejme.com/article/criminological-analysis-of-determinants-of-cybercrime-technologies

Temple, W. G., Wu, Y., Cheh, C., Li, Y., Chen, B., Kalbarczyk, Z. T., … Nicol, D. (2023). CyberSAGE: The Cyber Security Argument Graph Evaluation Tool. *Empirical Software Engineering*, *28*(1). https://doi.org/10.1007/s10664-021-10056-8

Tenis, A. A. & Santhosh, R. (2022). Challenges and Security Issues of Online Social Networks (OSN). *Notes on Data Engineering and Communications Technologies*, *68*, 703–709. Retrieved from https://www.semanticscholar.org/paper/Challenges-and-Security-Issues-of-Online-Social-Tenis-Santhosh/cd6f47cc532f6aafbd7e59935be4e22b795d84ca accessed on October 31, 2023.

The White House. Presidential Policy Directive--United States Cyber Incident Coordination. , Pub. L. No. Presidential Policy Directive/PPD-41, (2016). United States: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

Tongkachok, K., Apinawatawornkul, K., Promsaka, T., & Sakolnakorn, N. (2021). Legal Response in Thailand When Facing Cybercrime. *Journal of Legal, Ethical and Regulatory Issues*, *24*(1), 1–6. Retrieved from https://www.abacademies.org/articles/legal-response-in-thailand-when-facing-cybercrime-10979.html

United States Census Bureau. (2023). U.S. Population Trends Return to Pre-Pandemic Norms as

More States Gain Population. Retrieved August 3, 2023, from https://www.census.gov/newsroom/press-releases/2023/population-trends-return-to-pre-pandemic-norms.html

Wahid, A. A. (2020). Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi. *Jurnal Ilmu-Ilmu Informatika Dan Manajemen STMIK*, (November), 1–5. Retrieved from https://www.researchgate.net/publication/346397070_analisis_metode_waterfall_untuk_pengembangan_sistem_informasi

West Java Regional Revenue Agency. (2017). Jenis Cybercrime Berdasarkan Motif dan Aktivitasnya. Retrieved August 15, 2023, from https://bapenda.jabarprov.go.id/2017/11/10/jenis-cybercrime-berdasarkan-motif-dan-aktivitasnya/ website: https://bapenda.jabarprov.go.id/2017/11/10/jenis-cybercrime-berdasarkan-motif-dan-aktivitasnya/

Widakuswara, P. (2023). US Launches Aggressive National Cybersecurity Strategy. Retrieved December 1, 2023, from VOA website: https://www.voanews.com/a/us-launches-aggressive-national-cybersecurity-strategy-/6986279.html

Yuvaraj, & Venkatanarayanan, S. (2019). Analysis of Cybercrime as the Object of a Criminal Investigation. *Journal of Advanced Research in Dynamical and Control Systems*, *11*(4 Special Issue), 280–284. https://jardcs.org/abstract.php?id=502