MANU Bil. 34 (2), 1-16, 2023 (Disember)
E-ISSN 2590-4086

ANALYSIS OF INDONESIAN AND EUROPEAN UNION (EU) RELATIONSHIP STRATEGY OVERCOMING CYBER TERRORISM

[1]IBAADURRAHMAN AZZAHIDI
[2*]FRANSISKA MARISTELLA JUNIANSE

[1&2]Master of International Relations Study Program,
Universitas Muhammadiyah Yogyakarta, Brawijaya Street, Bantul, Yogyakarta, Indonesia
*Corresponding author: [*1]ninjasukarame@gmail.com*
Date Received: 18 March 2023 | Date Accepted: 21 August 2023 | Date Published: 1 December 2023
DOI: https://doi.org/10.51200/manu.v34i2.4767

Abstract This research discusses Indonesian National Security in handling entry of malware caused by the attack including cyber terrorism. Utilization Technology Increasing information and communication development has changed pattern groups certain to do actions that harm the media and cyberspace, it is known as cyber-terrorism. This research discusses cooperation between Indonesia and the EU in the field of cyber security and the emergence of cyber-terrorism in Indonesia. This research uses the theory of Cyber Terrorism and National Security from Ryan Cooper as a framework think. Besides that, this research uses method qualitative use studies literature with several sources related. The results of this study show that the European Union Convention on Cyber Terrorism as Regime International has proven to encourage Indonesia to make a constitution about security for Cyber terrorism as stated in Article 21 of the ITE Law. Cyberterrorism is qualified as a transnational Crime which refers to Article 3 of the United Nations Conventions against Transnational crime.

Keywords: Peace study, policy overseas, Indonesia, computer-aided methods.

INTRODUCTION

The threat posed by cyberterrorism has confiscate mass media attention that is community security and industry technology information. Journalists, politicians, and experts in various field has popularize a sophisticated scenario cyber terrorism in a manner electronic breaking into controlling

computer dam or control them cross air system, bring havoc and danger, not only millions life but also security national self. However, regardless from all prediction gloomy about cyber-generated apocalypse, no one example of real cyberterrorism has noted.

Cyberterrorism raises enough threat big so that must get attention special. Because in part big infrastructure critical in Western society is connected through computer, potential threat from cyberterrorism, of course just very apprehensive. Hackers, though no motivated by the same inspiring goals terrorists, have shown that individual can obtain access to information sensitive and operative service important. Terrorists, at least in theory, with thereby can follow traces of the hackers and then, break in government and private system computer, disable, or at least disable sector military, financial, and services economy forward. The more magnitude dependency public we to technology information has create form vulnerability new, give terrorist chance for approaching that target if no will truly not shake, like system defence national and air system control then cross. The more proceed technology a country, increasingly prone to attack cyber to the infrastructure.

Worries about potency the danger posed by cyberterrorism with thereby reasoned although right. However, no means that all fears that have voiced in the media, in Congress, and in public forums other rational and enter sense. A number of afraid no can justify, while others are so exaggerated. Besides that's the difference between potential and damage actual ones inflicted by cyberterrorists too often neglected, and relative activity benign part big hacker has combined with the spectre of pure cyberterrorism.

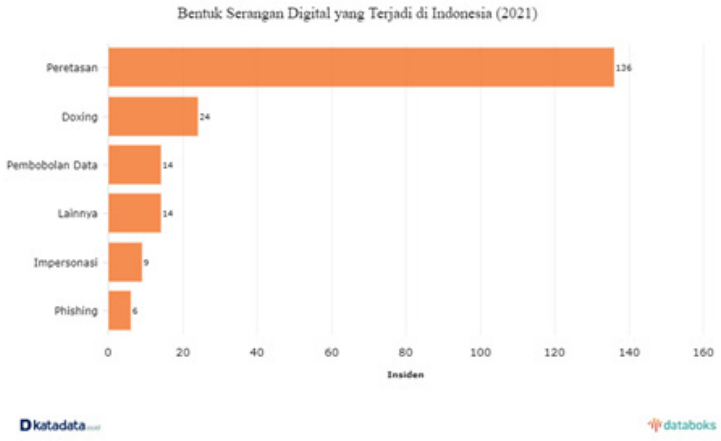
This report examines reality cyberterrorism threats, present and future. He started with decipher why worry *cyberterrorism* has gripping so many people, define what fulfil condition as "cyberterrorism" and what not, and mapped power pull terrorist cyberterrorism. Report the see evidence for and against Western society vulnerability to cyber-attacks, based on various research and publications latest illustrate type fears that have disclosed and for evaluate is we need do it so worried. In conclusion see into the future and argue that we must still alert danger real temporary no fall victim to fear excessive.

Work the European Union-Indonesia in problem security. In meeting the second split party discuss various covering issues war oppose terrorism and extremism violence, fight narcotics, maintenance peace and management crisis, security maritime, cyber security, non-proliferation, and management disaster. The EU and Indonesia noted good progress with implementation partnership they during several years last. In the fields counterterrorism and security cyber, EU and Indonesia held online workshop for share information and practice best covering issues like protection and treatment to related children with group terrorist, increase use technology finances and relationships with funding terrorists, fight narrative extremist force, and steps build trust in cyberspace. The EU and Indonesia also confirmed return commitment work the same they in a deep multilateral platform field this.

The dialogue is also shared challenges faced by the EU and Indonesia in oppose narcotics and discuss ways for strengthen response policy they through policy counter measures comprehensive narcotics, including rehabilitation. In the fields maintenance peace and management crisis, the EU and Indonesia stressed importance promote woman's role in operation peace while in the field security maritime, second split party emphasize importance work the same in awareness situation maritime. Both the EU and Indonesia are very attaching importance success conference review the 10th Agreement on Non-Proliferation Weapon Nuclear (NPT). For face Chemical, Biological, Radiological and Nuclear (CBRN) hazards, the EU and Indonesia highlighted work the same they are below Center of Excellence Initiative Mitigation EU chemical, biological, radiological, and nuclear risks. EU and Indonesia will continue work the same tightly they in problem consular including in context the COVID-19 pandemic. Finally, the EU and Indonesia compiled a list of activities work in the future in the areas discussed during Dialogue.

One form threat security cyber appear in form hacking that occurs in cyberspace, and faced by the government regions, companies, and citizens. The problem is hacking, espionage, or another cyber-attack can very damage without cause death or destruction in the real world. This become focus new in security and defence national including Indonesia, which is a country with most internet users.

Table 1 The digital attack that happened in Indonesia 2021

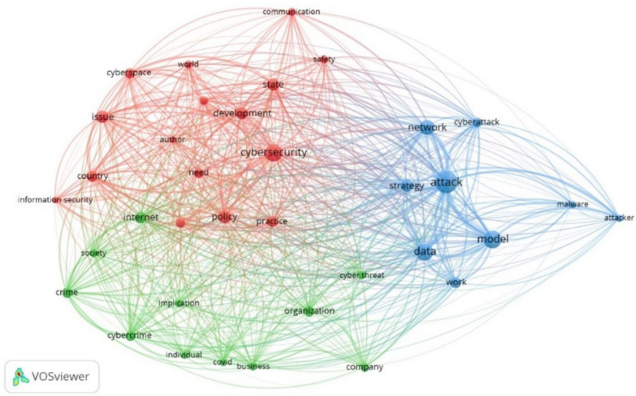


According to the US *Office of the Director of National Intelligence 2021 Annual Threat Assessment,* "Russia Keep going target infrastructure important, including cable underwater and systems control industry, in the US and in allied and partner countries, along the way enhancement compromised infrastructure and deep a number of cases can show ability for damage infrastructure during crisis." Assessment the state that Russia almost certain consider cyber-attack as possible options accepted for prevent enemy, control escalation, and sue conflict as well as operation chain supply device soft Russia oppose company technology US- based Information (IT) reveals about 18,000 customers worldwide, including network companies all over US Federal, state, and local governments; entity infrastructure important; and organization sector private other. Actors continue activity advanced for compromise system a number of customers, including a number of institution The US Government (Director of National Intelligence, 2021).

According to report from CISA (2022), invasion Russia to Ukraine can impact on the organization good inside nor outside area, including malicious cyber activity to US homeland, including as response on cost the economy yet once happen previously imposed on Russia by the US and allies as well as our partners. Every organization good big nor small must ready respond disturbing cyber incident. As the country's cyber defence agency, CISA is ready help organization prepare, respond, and mitigate impact cyber-attack.

Moment cyber incidents reported with hurry up, we got it use this information for give help and as warning for prevent organizations and other entities fall victim to attacks similar. CISA continues push stakeholders our interest to in a manner volunteer share information about incident related to virtual worlds that can help reduce threat current or new cyber security appear to infrastructure important (Cybersecurity & Infrastructure Security Agency, 2022) .

With using supporting software VosViewers, this study retrieves data from Scopus and some article scientific other than connected through system with VOSviewer. Superiority from the Scopus database can display system correlation (correlation) between articles and publications, as well as collaboration interauthor. Meaningful collaboration cooperates between more from one person or more from one institution in an activity, fine activity study nor education. After review further, we get the data, yet lots research yet discusses about topic this in a manner specific. However, these events increase US sensitivity to threat cybercrime against US sovereignty and security by Russia. This writing aim for analyze strategy security cyber in US as response to threat cyber-Russia.



THEORETICAL FRAMEWORK

1. Cyber-terrorism

There are some stumbling blocks for create clear and consistent definition from the term "cyberterrorism." First, like just mentioned, a lot of discussion about cyberterrorism has been done in popular media, where journalists usually fighting for drama and sensation than definition good operational from new terms. Second, very general when face to face with computer for create new words only with placing the word "cyber", "computer ", or "information" before another word. With thus, throughout word warehouse— cybercrime, info war, war network, cyberterrorism, cyber harassment, virtual warfare, digital terrorism, cyber tactics, war computers, cyberattacks, and cyber breaches— are used to describe what some have described military and political strategist as " "terrorism new " in our time.

Luckily, some effort has done for introduce accuracy more semantics big. Dorothy Denning, a professor knowledge computer, have put forward very definition no ambiguous in lot of articles and in his testimony about problem this is in front The House Armed Services Committee in May 2000: *Cyberterrorism* is meeting between cyberspace and terrorism. This refers to a breaking attack laws and threats attack to computers, networks and the information stored on them when done for intimidating or force government or the people in advance objective political or social. Next, for fulfil condition as cyberterrorism*,* an attack must result violence to people or property, or at least cause enough danger for cause fear. Attack that causes death or injury body, explosion, or loss dire economy will become for example. Attack serious to infrastructure important can become acts of cyberterrorism, depending on their impact. Annoying attack service that is not important or some big is expensive glitches do not will happen.

Important for differentiate between cyberterrorism and "*hacktivism,*" a term coined by scholars. For describe marriage hack with activism politics ("*hacktivism*" here understood as activities carried out online and covertly that copes disclose, manipulate, or exploit vulnerability in system operation computers and devices soft other. No like hacker, hacker tend not have a political agenda). Hackers own four weapon their main have: virtual blockade; e-mail attacks; hacking and burglary computer; and computer viruses and worms.

Virtual blockade is virtual version of sit -in or blockade physical: activist political visit the website and attempt produce so lots then cross to the site so that other users do not can reach it, so bother normal operation while win publicity through media reports for reasons for the protesters. "Swarming" occurs when a number big individual in a manner together access a website, cause its collapse. Crowds can strengthen effect weapon the two hackers: the campaign email bombing bombarding the target with thousand messages at once, is also known as a "ping attack".

The result startling organizer. First, the Red Team has shown that system command -and- control US military Pacific can penetrate and, potentially, immobilize it on the spot second, found NSA officials who checked results test that lot of infrastructure sector private sector in the US, such as network telecommunications and power electricity, got with easy attacked and abused with the same way.

Vulnerability industry energy was the essence of Black Ice. Verton argue that sector American energy will be the first domino to fall in attack strategic cyberterrorist against the US. Book this explore in terrifying detail how impact attack sort of that can rival, or even exceed, consequence from attack more physical traditional. Verton claim that for one year particular, the company average utility big in the US experience about 1 million cyber interferences. Data collected by Riptech, Inc.—a Virginia- based, specialized company in security online information and systems finance —on cyberattacks during six months after the 9/11 attacks showed that company in the industry energy experience intrusion double compared to industry another, with amount attack critical or critical need intervention soon averaged 12.5 per company. Deregulation and increase focus on profitability has make utilities and other companies increasingly Lots move operation they to the Internet for look for more efficiency bigger and more expensive low. Verton argues that industry energy and lots sector other has be a potential target for various cyber interference with make Internet link (physique nor wireless) between network them and the system control surveillance and data acquisition (SCADA). This SCADA system manage genre electricity and natural gas as well as control various systems and facilities industry, including factory processing chemistry, surgery water

purification and water delivery facilities wastewater management, and a number company manufacturing. Ability a terrorist for control, interfere with, or change function command and monitoring done by the system. This can threaten regional security and maybe national.

According to Symantec, one leader world company in the field security cyber, vulnerability new to attack cyber always found. Company reports that number of "holes device soft" (gap security device possible software hacker wicked for exploit system) grows by 80 per cent in 2002. However, Symantec claims that no there is not a single recorded cyberterrorist attack (implement definition that attack sort of that must originate from the incoming country on the watch list terror Department Overseas). This possible reflect fact that terrorist not yet own required knowledge. Alternatively, this possible describe that hacker no sympathetic to the cause organization terrorists — however, if second group join, result can destroy.

The same worry about it is prospects for terrorists that alone designing device soft computer for government agencies. Incredibly, as Denning explains in "Is Cyber Terror Next? "at least one example from situation like that is known has happens: In the month March 2000, the Japanese Metropolitan Police Department report that device soft.

System that has they get for tracking 150 vehicles police, including car not marked, has developed by the cult Aum Shinryko, the same group that did the gas on the trains lower Tokyo lands in 1995, killing 12 people and injuring 6,000 others. At the moment invention, cult the has receive tracking data secrets on 115 vehicles. Next, cult has developed device soft. For at least 80 companies Japan and 10 institutions government. They have work as subcontractor. For other companies, so almost no possible for organization for know who developed device soft. As subcontractor, cult they can install Trojan horse for launch or facilitate attack cyber terrorists later day.

2. National Security

Based on various literature, security national in a manner general interpreted as need base For protect and guard interest national something sovereign nation with use strength political, economic and military For face various threat well come from outside nor domestically (Ryan et al., 2006) .

Interest national then become the dominant factor in draft security national something nation. Security national too interpreted as need for maintain and maintain state existence through strength economic, military, and political as well as development diplomacy. Draft this emphasize to ability government in protect the territorial integrity of the state of incoming threats from outside and from within the country. Security national as something draft often experience change because exists constellation political international. Define security national no something easy, because that in framework law international submitted to each country, with notes no violate concept of democracy.

National security theory is gathering related knowledge with draft security national, and the strategy used government and institutions for ensure safety and welfare its citizens. Field theory security national characteristic interdisciplinary and encompassing various discipline science, including knowledge politics, relationships international affairs, military strategy, and studies intelligence. In essence, theory security national try understands characteristic threat to security a country, including threat military, political, economic, social, and environmental. It also copes identify strategies and policies that can used government and institutions for prevent or reduce threat this. Theory security national has develop from time to time for reflect change landscape global politics and emergence threat new to security national. For example, in the post 9/11 era, national security theory more emphasizes non-traditional threats, such as terrorism and cyberattacks.

A number of draft keys in theory security national includes deterrence, defense, and pre-emption. Prevention involves use of military strategy or diplomatic for prevent enemy act aggressive. Defense refers to the steps taken government for protect its territory, citizens, and institutions from

attack. Pre-emption involves acting proactive for prevent enemy do planned attack. Kindly whole, theory security national give framework work for understand landscape threat to security complex national and always change and for develop an effective strategy for get over it.

Based on various literature, security national in a manner general interpreted as need base for protect and guard interest national something sovereign nation with use strength political, economic, and military for face various threat well come from outside nor domestic. Interest national then become the dominant factor in draft security national something nation. Security national too interpreted as need for maintain and maintain state existence through strength economic, military, and political as well as development diplomacy. Draft this emphasize to ability government in protect the territorial integrity of the state of incoming threats from outside and from within the country. Security national as something draft often experience change because exists constellation political international. Define security national no something easy, because that in framework law international submitted to each country, with notes no violate concept of democracy.

Definition security national keep going debated because exists differences and similarities among experts. According to Berkowitz, security national can very develop defined as ability from one nation for protect values internal from threat outsiders. Concept this more lots growing in the US post World War II, which started focus to ability military, then develop to various matters of a non-military nature. In addition to Berkowitz, Arnold Wolfers in 1952 stated, that security refer to level protection to the previous values achieved. Arnold Wolfers argues that security own connection with hope. Connection between both of them namely, security own interest no only protection from the previous values achieved, but also the future expectations and results that are of value enjoyed then day (Wolfers, 1952).

Finally, security is also minimized threat. Threat can see as anticipation to barrier from a number of value when we speak protection usually discuss about free from barriers and hindrances to what to enjoy as valuable results. Interest national finally become security with refers to results value that those who have it desire on an effective basis political something nation.

METHODOLOGY

This study uses methodology study qualitative with object study focused on writings that have been published in journals national nor international. Study this too is descriptive for explain meaning and substance war cyber that alone as well as solution for Indonesian nation in address war cyber. This is study beginning related issue war cyber so that study this is study conceptual things studied from study this is around meaning, and form from war cyber as well as possible solution carried out by the State of Indonesia in face threat war cyber. Expected study this can destroy confusion we in interpret war cyber, also helps all party for more understand in a manner deep form threat or challenge from war cyber as well as possible alternative thinking made as answer solutions, for Indonesian nation in face threat or challenge war cyber that alone.

RESULTS AND DISCUSSION

Security Development of Indonesian at continues National Movement with based on the values of Pancasila as a way of life because become the basic idea that is conceptualized in the opening of the 1945 Constitution of the Republic of Indonesia and Batang The body of the 1945 NRI Constitution. After conceptualizing the idea then form regulated system in Regulation Legislation, this (system) must be next construction in a manner substance, structure, and culture. System security built national must target to fourth room scope security national namely, security exit; security to in; security public; and security human (Ananakotta & Disemadi, 2020).

1. Indonesia Strategies to Combat Cyber Terrorism

Revolution in the field technology information and communication has given benefit or meaningful wisdom for world community for interact, however matter it also set aside problem new form threat war cyber. Jan Kalberg says that there is four necessary thing anticipated from war cyber first; his enemy anonymous, second; the object fixed, third; result measurable, and fourth; the execution fast. In his writing, M. Badri (2012: 104) explains that war cyber vulnerable to countries and communities that do development technology

electromagnetics and technology information and communication. According to him war cyber not only war in cyberspace for attack personnel, facilities or equipment information and computers, however become part of information operations (IO) which includes it is operation psychological, deception military, operations security, war suspected electronics and computer network operations (CNO). As something action use computer network for attack systems and networks information society. Theory used in war strategy cybers based on Dr. J. Kallberg (2016: 13) is create instability in the target country, thus war cyber can said succeed if capable remove capacity military or create destabilization society in the target country. In matter this so orientation war cyber is weaken institution so that public become no stable, and in the end state condition to be weak, and when the state becomes weak, then the country will tend submit to power foreign. In view strategic, war cyber only used in support operation military and geopolitical, therefore that said by Martin Libicki that cyber war is not it is standing mechanism alone in war, however there is intimate correlation between war cyber and power others (Jan Kallberg, Kallberg, 2016: 119).

Cyberterrorism is growing threats in Indonesia, and the government has applied some strategies for fight it. Following is some of the main strategies:

a. Strengthen infrastructure security cyber, the Government of Indonesia has work for increase infrastructure security cyber with to form the National Cyber and Crypto Agency (BSSN) for develop policies and guidelines security cyber, as well coordinate effort security cyber in between various institution government.
b. Cybercrime Law, Indonesia has passed the Cybercrime Law (UU ITE) which criminalizes activity like hacking, deploying information false, and seditious hatred online. Constitution it also regulates work the same between institution enforcer law and providers internet service for track cyber criminals.
c. Campaign Awareness Public: The Government of Indonesia has launch campaign awareness public to educate public about cyber threats and push they for practice safe online behaviour. This campaign covers information about method recognize phishing scams, avoid malware download, and protect information personal. International Cooperation: Indonesia has involved in cooperation

international for combat cyber terrorism, including participate in exercise together with other countries and share information and practice best with organization international.

d. Monitoring and detection, the Government of Indonesia has formed the Cyber Threat Intelligence Center (CTIC) to monitor and detect cyber threat. CTIC is working the same with institution government other for investigate and respond cyber-attack. Kindly overall approach Indonesian government for combat cyber terrorism involves combination development infrastructure, framework law, education public, work the same international, as well monitoring and detection. This effort very important for protect country's digital infrastructure and ensure safety and security its citizens.

2. Cooperation between Indonesia and the European Union

Indonesia and the European Union (EU) have collaborated in security cyber in various way. In 2019, Indonesia and the EU signed a Memorandum of Understanding (MoU) for strengthen work the same in security cyber and data protection. The MoU covers fields like share information, various field like management incident, exchange information, upgrade capacity, research security cyber, and work the same in development policy.

As apart from this cooperations, the EU has support Indonesia in increase ability security the cyber through various initiative. As example, in 2020, the EU provides funding for Capacity Building Project ASEAN-EU Cyber, which aims for increase readiness security cyber of ASEAN member countries, including Indonesia. One field main work the same between Indonesia and the EU is development policies and regulations security cyber. EU has share experience and practice the best with Indonesia regarding issues like data protection and privacy, standard security cyber, and management risk security cyber.

Besides work bilateral cooperation between Indonesia and the EU, Indonesia also became member of the ASEAN (Association of Southeast Asian Nations) Regional Forum on Cybersecurity (ARF-CSC), which provides a platform for work same inner region issue security cyber. EU

itself already become active participant in ARF-CSC, delivers help technical and support development capacity to ASEAN member countries, including Indonesia. Besides In addition, Indonesia and the EU have also worked the same for increase capacity institution enforcer law and rulers interest related other for overcome threat security cyber. This including giving training and technical assistance to institution enforcer law, as well support security strategy development cyber national for Indonesia.

Kindly overall, cooperations between Indonesia and the EU in the major of security cyber reflect increasing confession will importance collaboration international in overcome characteristic threat increasingly cyber complex and interrelated cyber threat.

CONCLUSION

Indonesian still very prone to attack cyber. Basic stuff is because first, Indonesia is not a developed and rich country. Second, technological information and telecommunication we still depending on developed countries with owner's patent technology. Third Indonesia only consumer or user internet services with very high percentage high. Fourth in Indonesia yet build a defense system cyber for can anticipate all possibility can happening war cyber. War cyber is war necessary moderation anticipated with all comprehensive analysis, therefore based on conditions, and positioning from Indonesia itself, then Indonesia needs do development security cyber/ cyber security with multiple approaches and implemented in a manner comprehensive and professional. Indonesia also needs do cooperation at the international, regional, tri and bilateral levels for face threat war cyber from state actors as well trans international community.

Security cyber for Indonesia is necessary become part from focus structure international, so policy that they made was emphasized in system as part from norm international. In this matter, policy security Indonesian National show necessity protection to inhabitant his country more improved because will harm the country, however in more context far policy. This is effort Indonesia for create norm new in system about security cyber.

This research reaches out a number of literatures related regarding with state security and security cyber, then from that writer appeal to research furthermore for discuss decisions taken by Indonesia and the EU with different approach.

REFERENCES

Anakotta, MY, & Disemadi, HS (2020). Continuing system development internal Indonesian National Security coping system legal framework crime terrorism. *Journal National Security2, VI* (1), 41–71.

Babys, Sam (2021). Threat war cyber in the digital era and Indonesian security solutions. *Journal Oratio Directa, 3* (1), 425–442. https://ejurnal.ubk.ac.id/index.php/oratio/article/view/163

Banyász, P. (2014). Act as a spy - The Edward Snowden Case. Management teória, výučba a prax, (pp. 194-201). Liptovský Mikuláš.

BBC. (13 July 2018). Two twelve Russian syndicated on hack US election 2016. Retrieved from BBC News: https://www.bbc.com/news/world-us-canada44825345

Brenner, SW. (2002). Cyberterrorism. Asia Media, 29(3), 149–154. https://doi.org/10.1080/01296612.2002.11726680

Cisco. (20 December 2022). What is Malware? Obtained from Cisco: https://www.cisco.com/c/en/us/products/security/advanced-malwareprotection/what-ismalware.html#~related-topics

Commando, US C. (2018). Achieve and Maintain Vision Command Virtual World Excellence for US Cyber Command. Obtained from US Cyber Command: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

Command, UC (12 December 2021). Our history. Obtained from US Cyber Order: https://www.cybercom.mil/About/History/

Crumpler, W., & Lewis, JA (2019). Labor Gap *Cyber security.* CSIS,

Center for Strategic and International Studies.

Defence, D.O. (2018). *Security Strategy Cyber Department Defense*. Obtained from Department Defense, United States of America. https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/Cyberstrategysummaryfinal.Pdf

Defense. (2020). DoD Data Strategy. Taken from https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/Dod-Data-Strategy.Pdf

Fidler, DP. (2016). Us Election Hacks, Cybersecurity, and International Law. *American Journal of International Law (AJIL) No Bound*, *110*, 337-342.

Galinec, D., Možnik, D., & Guberina, B. (2017). Security Cyber and Defense Cyber: Approach National Level Strategy. Automats. *Journal Control, Measurement, Electronics, Computing and Communication,* 273286.

Ghernaouti, S. (2013). *Cyber Power Crime, Conflict and Security in Cyberspace*. EPFL Press.

Holsti, KJ, & Cliff, E. (1967). *Political International: Framework Analysis*. Prentice Hall.

Holsti, KJ, Monterichard, M., Msabaha, I., Robinson, TW, Shaw, T., & Home, TW. (2018). United States National Cyber Strategy. Obtained from the US White House: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Home, W. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/rssviewer/internationalstrateg yforcyberspace.pdf

Mintz, A., & Jr., KD. (2010). *Understanding policy decisions overseas make*. Cambridge University Press.

Patton, MQ, & Cochran, M. (2002). *Usage guide methodology study qualitative*. Officer MSF Research.

Research, CE. (20 October 2022). Fast facts hacking campaign President 2016 gained from CNN https://edition.cnn.com/2016/12/26/us/2016presidential-campaign-hacking-fast-facts/index.html

Ryan, Cooper, & Tauer. (2006). Programming for peace: Computer-aided methods for international conflict resolution and Prevention. In R. Trappl (Ed.), *Paper Knowledge. Toward a Media History of Documents.* Springer Netherlands. https://doi.org/10.1007/1-4020-4390-2

Sanger, DE. (13 December 2021). Hacker Russia breaks into Federal Agency, suspect US officials. Taken from The New York Times: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-usgovernment-treasury-commerce.html

Security, UD. (7 October 2016). Joint Statement of Department Security Home Affairs and Director's Office National Intelligence for Security election. Obtained from Department Security US Homeland: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

Statistics, CS. (15 October 2021). Statistics Cyber Security. Obtained from Statistics Cyber Security: https://purplesec.us/resources/cyber-security-statistics/

Warner, M. (2020). Decade First Command US Cyber. Hoover Institution Essays.

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol. *Political Science Quarterly, 67* (4), 481. https://doi.org/10.2307/2145138

Zylberberg, J. (2016). Why the nation reassembles: Restructuring policy abroad in the postwar world. Routledge.