Cyberwarfare Readiness in the Maritime Environment

Diop Ausar Harris
Department of Electrical Engineering and Cyber Systems, United States Coast Guard Academy, New London, Connecticut, U.S.A.

Keywords: Cybersecurity, Cyberwarfare, Information Systems, Maritime Environment, Port Security.

Abstract: Cybersecurity ensures that sensitive information and data are protected. Even so, there are still roadblocks that impede an organization's ability to uphold cybersecurity. This study provides an analysis of challenges present in the maritime environment that may impede the preparedness of cyberwarfare. The research showed that the United States tends to be more vulnerable to cyberattacks due to its dependence on information technologies. Numerous cases also showed that the United States, compared to other powers, lacks somewhat in defensive capabilities. Many of the breaches in cybersecurity were due to a lack of cyber awareness leading to human error accidents. Vessels and ports are also likely targets during a cyberwar due to their importance in a country's economy and security. These challenges present in the maritime environment must be dealt with to prepare for a potential cyberwar. For effective cyberwarfare readiness moving forward, states should aim to increase cybersecurity awareness, improve capabilities, and promote cooperation between states. Proposition for continued research on cyberwarfare readiness in the maritime environment by academic researchers and practitioners is recommended.

1 INTRODUCTION

Cyberspace is practically the newest frontier. Like the sea and airspace in the past, the discussion of how cyberspace can be used and regulated is a huge topic. This makes sense, as cyberspace is evolving so rapidly that many issues and challenges arise. The cyberspace domain consists of numerous systems such as satellites, computers, Wi-Fi, storage devices, and many other systems we utilize every day (Junio, 2013). However, the increased utilization of cyberspace creates a threat that those in the past would never have even imagined, the prospect of cyberwarfare.

Cyberwarfare can be described as a war conducted in and from computers as well as the networks connecting them, waged by states or their proxies against another or multiple states (Streeter, 2013). A cyberwar today would be tremendously expensive whether it is deadly or not. The likelihood of attacks is also increasing as countries develop and advance their cyber capabilities (Korstanje, 2016). With the world becoming more dependent on cyber and information technology (IT), the prospect of a cyberwar being prominent in future conflicts is a growing concern that calls for serious attention.

Cyberwarfare threatens numerous industries and domains that are essential for our society to function. One of these is the maritime environment. Ports and terminals are critical infrastructures, which make them prime targets for cyberwarfare attacks (de la Peña Zarzuelo, 2021). There are currently numerous naval forces and maritime security organizations that maintain security both on and off the homeland. There are still existing challenges that could prevent the maritime environment from being prepared for cyberwarfare. However, proper action can be taken to resolve these issues by examining these roadblocks and information systems.

2 METHODOLOGY

The main purpose of this paper is to identify the current state of the maritime environment when it comes to cyberwarfare readiness. The paper also seeks to emphasize the need for a greater focus on cyberwarfare readiness in the maritime environment, and what actions and plans can be practiced in the future to ensure the domain is ready for potential conflict.

To gain an understanding of the maritime environment's current readiness for cyberwar, as well as developing potential solutions to build upon certain areas, sources that explained cyberwarfare and how it threatens national security were used. This involved

Harris, D.
Cyberwarfare Readiness in the Maritime Environment.
DOI: 10.5220/0011068400003179
In *Proceedings of the 24th International Conference on Enterprise Information Systems (ICEIS 2022) - Volume 2*, pages 119-125
ISBN: 978-989-758-569-2; ISSN: 2184-4992

looking at both the technical and international political sides of cyberwar. Librarian databases were used to look for sources that could be beneficial. Scholarly websites were utilized to search for empirical studies that would help analyze the maritime environment and cyberspace more in-depth providing analysis and data. Internet search systems were also used to find general sources that could provide some facts or insight on the topic of the maritime environment's readiness and cyber, and what roadblocks commonly found in organizations can impede their readiness. All of this resulted in initiating research and a better understanding of the increasing concerns of cyberwarfare in the maritime environment.

3 FINDINGS

3.1 Dangerous Components

Cyberwarfare is on the rise due to numerous components of the nature of cyber-attacks and cyberspace. Five reasons are the vulnerability of the Internet, high return on investments, inadequate cyber defenses, plausible deniability, and the participation of non-state actors (Green, 2015). Attacks like Stuxnet have shown the world that cyber-attacks can be extremely sophisticated. Stuxnet was very selective about its choice of target, unlike most earlier worms before it. It was aimed specifically at a physical and military target, while also being specific about the conditions of the targets (Chen, 2010). It also has been reported to have unusually complex code, large size for malware, and written in multiple languages (Cyber Threat Source Descriptions, n.d.). Stuxnet is estimated to have infected 50,000–100,000 computers (Chen, 2010).

Another incident that showed that United States (U.S.) systems were vulnerable was Solar Sunrise. In February 1998, numerous Department of Defense (DoD) networks were attacked due to the exploitation of a well-known vulnerability in the Solaris computer system. The attackers had the goal of planting a program to gather and later collect data. Despite the attackers only having moderately sophisticated tools, over 500 computer systems were compromised. While the Justice Department claimed that no classified information has compromised during this attack, the incident showed that U.S. information systems can very quickly be compromised, putting the national security of the U.S. at risk (Johnson, 2015).

Another concern of cyber-attacks is that they often bring indirect effects once they are executed. Attacks can bring collateral damage to those who may not even have been intended to be affected, as the attacks have a large radius of effects. These attacks are highly unpredictable, as there are numerous ways they can behave and could have unforeseen consequences. Cyber-attacks are also known for their direct effects bringing short-term reversible effects, but indirect ones causing damage that usually is irreversible. They can have dire consequences that indirectly disrupt real-world missions and tasks that could put lives at risk (Parks & Duggan, 2011).

There are numerous similarities between securing cyberspace to the sea and airspace. The sea was largely secured in the nineteenth century, while airspace was the main domain actively being secured and discussed in the twentieth. Global powers now wish to do the same with cyberspace. They wish for it to become more secure for people and businesses to operate in. Cyberspace however is ungovernable in nature, as it constantly evolves at a fast pace. Many threats could also hide in cyberspace without governments being able to identify them. It is both inevitably threatening and inhabited by unknown antagonists. Not to mention the fact that the more dependent states become on information systems, the more vulnerable they become to information warfare. These aspects of cyber security discourse prove that the domain is both unique and unpredictable (Boyes, 2014).

3.2 Foreign Organizations and Governments

National cyberwarfare programs pose an enormous threat to global interests, especially regarding the maritime environment. Among the array of cyber threats, it is mainly government-sponsored programs that are developing capabilities with the prospect of causing extensive and long-duration damage to U.S. critical infrastructures (Daum, 2019). Statistics show that 26.3% of all cyberwarfare strikes are directed to the U.S. (Cvetićanin, 2020). The number of cyber-attacks in the U.S. and other countries will likely increase in the future, as there was a large increase in cyberwarfare activities between 2009 and 2018, with attacks surging by 440% and currently showing no signs of slowing down (Cvetićanin, 2020). Many global organizations are also indicating that they are having difficulties dealing with cyber-attacks, and 20% of them consider global espionage their number-one threat (Cvetićanin, 2020). Another thing to note is that when it comes to the maritime domain and naval forces, the nature of cyberspace encourages the offensive military capabilities of the enemy, meaning

adversary states now have potentially dangerous weapons at their disposal (Dwarakish & Salim, 2015).

3.3 Importance of Maritime

The maritime industry is of great importance to the global economy. Marine transportation is 80% by volume of global trade and accounts for over 70% of its value (Chen, 2010). The maritime sector encompasses a wide range of services, such as the transportation of goods and people, various port services, and auxiliary or supporting services (Geers, 2008). As opposing powers often try to attack and compromise their enemy's resources, power, and wealth during wartime, the maritime environment would certainly be a prime target during a cyberwar.

3.4 Lack of Knowledge

An issue that cannot be ignored is the low level of cyber security awareness and culture within the maritime sector (DiRenzo, Drumhiller, & Roberts, 2017). A reason for this is that the maritime sector traditionally has only had to deal with physical domains in the past. However, information technology continues to grow important in the maritime sector every day. This reliance on the technology while beneficial for conducting operations also makes vessels and ports more exposed and vulnerable. If most individuals within the maritime sector are not aware of the danger of cyber-attacks, then it becomes difficult to effectively respond and develop mitigation plans.

A major weakness in our information technology systems can be mistakes done by people. Human error is a major contributing factor to cyber breaches in general. Over 90% of all cyber security breaches are caused by preventable employee errors in both the public and private sectors (Cvetićanin, 2020). Maritime workers need to have a good grasp on how cyber-attacks can threaten operations, and how cyber vulnerabilities can affect others both at sea and in ports. While maritime organizations have gotten better at addressing this issue, there still is a need for constant monitoring and improvements in the education of cyber security.

3.5 Global Navigation

One of the biggest threats that cyberwarfare presents to global navigation is Global Navigation Satellite Systems (GNSS) jamming and spoofing activities. It is estimated that around 87% of merchant vessels rely upon GNSS (DiRenzo, Drumhiller, & Roberts, 2017). Most countries today can jam GPS, and many such as North Korea have already done so (Dombrowski & Demchak, 2014). This indicates that using spoofing and jamming as tactics in war is very possible and could bring extremely disastrous results.

GNS Spoofing is when adversaries make a GPS receiver calculate incorrect positioning and timing information (Andronjna, Brcko, Pavic, & Greidanus, 2020). By sensing a similar yet slightly stronger signal, adversaries could easily take over vessels with GPS, confusing and directing them where they want. Spoofing has become easily available at the consumer level, with instructions and kits for building a spoofing device being offered for around $300 (Dombrowski & Demchak, 2014). With spoofing devices being easily assessable, numerous vessels could very well become vulnerable depending on the adversary's sophistication in technique and technology.

GNS Jamming differs from spoofing as it involves overpowering the GPS satellite signals locally so the receiver can no longer operate properly. GNSS jammers are normally illegal in the U.S., Canada, and Europe. However, it is still possible for jammers of various sizes and power ratings to be purchased off the internet. Due to this, GNS jamming devices are easily accessible to many, including enemies to the U.S. (DiRenzo, Drumhiller, & Roberts, 2017). Small-handed jammers are also normally difficult for law enforcement agencies to detect, as they can be used intermittently without being detected, are highly mobile, and can be disposed of quickly if needed (Dombrowski & Demchak, 2014). Many vessels primarily depend on GPS to navigate safely, and without it, would be at risk. Jamming can very well result in a ship's systems either failing or giving false and misleading information.

3.6 Port Security

Ports are integral to our economy. They are a very important component of marine transportation and the land transport chain. Port security against cyber risks is something that needs to always be maintained. However, there currently exist minimal clear standards and requirements addressing critical maritime infrastructure. Ports have been shown in past events to be almost effortless to penetrate. An example is the hacking of the Port of San Francisco, which relocated the port in cyberspace twenty miles north and became problematic in foggy weather. Due to their great importance to both the economy and national security, ports are a prime target for cyber-attacks during wartime. There is a dire need for

standardized policies for assessing, containing, and mitigating cyber risks (Andronjna, Brcko, Pavic, & Greidanus, 2020).

4 DISCUSSIONS

4.1 Increasing Cyber Awareness

The first course of action that needs to be taken is to further educate mariners. Human errors and misjudgments are the cause of most successful cyber-attacks (Hørthe, 2020). Lack of skill and lack of responsibilities by everyone are also common challenges that come with people (Teoh, Mahmood, & Dzazali, 2018).

Training and awareness are crucial to ensure people are educated and cyber security can be better maintained (The Three-Pillar Approach to Cyber Security: Data and Information Protection, 2020). Organizations have already begun promoting awareness of cyber security. This is a crucial step, because if the world does not acknowledge the dangers of cyberspace and the growing trend of attacks, then this incomprehension will act as a barrier and cause all to be susceptible. People must understand how the dangers of cyber-attacks and cyberwar differ from traditional threats. Cyberwarfare is unique due to being an evolving artificial world and deals more with versatility as opposed to mobility (Sheldon, 2016). Principles such as the lack of physical limitations, kinetic effects, stealth, mutability and inconsistency, identity and privileges, dual-use, and infrastructure control are tied to cyberwarfare. These attributes need to be acknowledged when not only building our capabilities but developing defenses against enemies as well (Saltzman, 2013). There can also be models developed based on research and analysis of past attacks. This makes it easier to determine the risk to help personnel with the assessment of dangerous scenarios (Albahar, 2019).

To ensure that cyber awareness training is continued to be improved upon, the Coast Guard could put more resources into the training and regulations on cyber-security. Standards on topics such as alcohol and fraternization are commonly known because they are frequently discussed in taught and discussed. Maritime workers are also used to what regulations and standards their vessels and ports are expected to uphold. Due to this consistency and accountability, people have a good understanding of what is expected of them, and this helps prevent potential situations where these rules would have been broken. The same needs to be done with cyberspace. Members need frequent discussions and education on the topic to ensure they are well equipped to deal with, respond accordingly, and enforce regulations in scenarios concerning cyberspace.

4.2 Further Developing Capabilities

Continuing to develop and improve upon our technology is also essential, as hardware and software capabilities can help guarantee reliable cyber security (What Are the 3 Pillars of Cyber Security? 2020). Upholding excellent offensive cyber capabilities allows a state to deter cyber-attacks and defend itself if necessary.

For deterrence of cyber-attacks to be successful, there must be the existence of capability (weapons), the credibility of the threat, and the capability to convey the threatening message to a potential opponent. The existence of capability makes it clear to both sides in a potential conflict that choosing to fight could come with a large cost. The weapon must be able to be used if needed, proving the credibility. The challenger must also be aware of the defender's willingness to use them if necessary (Nguyen, 2013). When needed, countries in times of war must have the capabilities to be able to support and work alongside their allies.

As states get attacked by any kind of attack, defenses built to counter them are expected to follow (Hildreth, 2001). Many argue that the offense always seems to be more advantageous than cyber defenses, as cyber-attacks are cheap, quick, and usually easier to carry out, while cyber defense on the other hand is a time-consuming and costly task that requires more proper knowledge. The U.S. fits this idea, as it is one of the most powerful countries when it comes to offensive cyber capabilities, but also one of the weakest ones defensively (Valeriano & Maness, 2018). The offense-defense balance concerns for cyberspace however are often exaggerated. Cyber offense does have numerous advantages when compared to cyber defense, such as speed and ease to do. However, cyber offense is checked by the inability to predict and control the consequences the attack may bring (Lupovici, 2011). Having both strong offensive and defensive cyber capabilities is essential for countries to protect themselves from threats.

The use of artificial intelligence (AI) and machine learning (ML) are possible ways to develop capabilities both offensively and defensively. Both methods help reduce human error, a common issue with maintaining cyber-security (Sobers, 2020). Both

are also adaptive, allowing them to be modified to fit the specific needs of ports and maritime organizations. Hackers can still however find ways to get around AI and ML algorithms. The algorithms can be deceived and even used maliciously for criminal purposes (Kuzlu, Fair, & Guler, 2021). Human oversight might still be necessary to ensure no drastic issues arise. Even so, with continuous research and development with the technology, AI and ML algorithms could help improve the security and cyberwarfare readiness of the maritime environment.

The U.S. Coast Guard could also play a huge role in addressing the major concern with GNSS. Since many vessels depend on GPS, Coast Guard inspectors can ensure that the vessel's receivers and antennas are structured and placed where they will have integrity in their monitoring. This can ensure that they are less likely to receive signals not from space. The Coast Guard could also work alongside the government to provide multiple GNSS. While these satellite signals may still be vulnerable, it would help mariners as they would have more than one GNSS that they can depend on (Dombrowski & Demchak, 2014). This could help reduce the danger that GNSS spoofing and jamming currently presents to the maritime environment.

4.3 International Discussion

Another course of action that could help the global maritime environment would have to be the discussion between states concerning cyberwarfare. Maritime organizations across the world can come together to express the concerns cyberwarfare presents and put plans in motion to counter this potential problem. The United Nations could discuss the topic and come up with viable solutions to prevent the unimaginable damage an all-out cyberwar could cause. This would be like nuclear deference, as many countries would discuss and make agreements to limit the spread and use of weapons. In a global world, the consequences of a cyber-attack affecting a single terminal can quickly spread to the entire supply chain and negatively affect many (de la Peña Zarzuelo, 2021). The use of cyber weapons for warfare threatens the entire world, and it is in everyone's benefit to come to an agreement on how to ensure the safety of the world is ensured (Valeriano & Maness, 2018).

An increase in the discussion between states about potential cyberwar could result in treaties being developed. The treaties would have the goal of decreasing or preventing the usage of cyber-attacks in various scenarios. While states may never hold a firm grasp on cyberspace and the technological components like other physical weapons, they may at least be able to make treaties that encourage states to utilize cyberspace in more peaceful matters. They may also seek to make treaties that allow states to cooperate in developing cyber defense systems combined with mitigation plans to better respond to attacks.

The execution of this strategy could help minimize the probability of cyberwar. This would not be easy, as the future is unknown since cyberspace is unpredictable and ever-changing. Therefore, constant education and training on how to protect our infrastructure need to be pushed heavily. Officials should bring these discussions up more often during official conferences and meetings. They must then make policies to help address concerns and ensure the citizens of the world stay protected. These processes must be constantly updated to ensure they can effectively reduce the risk from ever-changing cyber threats (Teoh, Mahmood, & Dzazali, 2018). Following through on all of this could be a big step in addressing the cyberwarfare dilemma.

4.4 Commitment from Leadership

To accomplish the prementioned actions, there needs to be a commitment from many leaders in state governments and maritime organizations. There must be a serious commitment for improvement for true progress to be made. Without leadership earnestly examining and being willing to address the issues concerning cyberwarfare readiness in the maritime environment, progress will be inconsistent (Bodeau, Graubart, & Fabius-Greene, 2010). Support from leadership will be needed to implement training and education, improve cyber capabilities, and set up discussions to ensure cyberwarfare preparedness.

5 CONCLUSION

Numerous roadblocks in the maritime environment have been identified and found to potentially harm the domain's readiness in a cyberwar. Many in the maritime environment are not fully aware of the dangers that cyberwarfare could bring. It is probably safe to assume for many, the thought has never crossed their mind. The increased dependence on vessels' electronic navigation systems may also be at a huge risk. While one may assume that a ship is essentially isolated at sea, modern-day ships are always communicating with a network and satellites. Spoofing or jamming attempts can render navigation systems useless and put many in potential danger.

Even ports due to their importance in a country's economy and overall stability become a prime target of cyber-attacks for wartime purposes.

Everything considered, there are plenty of actions that can be taken to address the roadblocks of cyberwarfare readiness. Improvements in education in the maritime environment have already been occurring, and as long as it is constantly reassessed and improved upon, can lead to having servicemembers more knowledgeable and ready for cyberwarfare. Making sure that naval forces have sufficient offensive and defensive cyber capabilities is also crucial. Developing and maintaining robust monitoring and response systems and capabilities is essential to protect national security (Lieber, 2014). Analyzing problems that are occurring, such as GNS spoofing and jamming, and coming up with methods to reduce or solve the issue, is also something that must be practiced. Cooperation between states to promote international rules of the road detailing appropriate conduct and regulations will also prove to be of benefit. All of this can be possible with the commitment of many of the leaders of governments and maritime organizations.

For future objectives, continued research by academic researchers and practitioners so further knowledge and action are achieved regarding cyberwarfare readiness in the maritime environment is suggested. Cyberspace is ungovernable in nature, as it constantly evolves at a fast pace. It is both inevitably threatening and inhabited by unknown antagonists. The domain is both unique and unpredictable. This however does not minimize the need for cyber-security practices. They instead may increase the need and desire to do so (Boyes, 2014). Constant attention to the changes in cyberspace, along with addressing arising challenges can help the maritime environment be better prepared for the possibility of cyberwar.

ACKNOWLEDGEMENTS

The completion of this research paper could not have been possible without the guidance of Dr. Angela Jackson-Summers, an Assistant Professor of Information Systems at the United States Coast Guard Academy.

REFERENCES

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. Science and Engineering Ethics, 25(4), 993-1006.

Andronjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8(10), 776.

Bodeau, D. J., Graubart, R., & Fabius-Greene, J. (2010, August). Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels. IEEE Second International Conference on Social Computing, 1147-1152.

Boyes, H. (2014, January). Maritime Cyber Security – Securing the Digital Seaways. Engineering & Technology Reference, 1(1).

Chen, T. M. (2010). Stuxnet, The Real Start of Cyber Warfare?[Editor's Note]. IEEE Network, 24(6), 2-3.

Cvetićanin, N. (2020, February 3). The Largest Battlefield in History – 30 Cyber Warfare Statistics. Retrieved January 20, 2022, from DataProt: https://dataprot.net/statistics/cyber-warfare-statistics/

Cyber Threat Source Descriptions. (n.d.). Retrieved March 17, 2021, from CISA: https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions

Daum, O. (2019). Cyber security in the Maritime Sector. Journal of Maritime Law and Commerce, 50, 1-19.

de la Peña Zarzuelo, I. (2021). Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on this Issue. Transport Policy, 100, 1-4.

DiRenzo, J., Drumhiller, N. K., & Roberts, F. S. (2017). Issues in Maritime Cyber Security. Westphalia Press.

Dombrowski, P., & Demchak, C. C. (2014). Cyber War, Cybered Conflict, and the Maritime Domain. Naval War College Review, 67(2), 70-96.

Dwarakish, G. S., & Salim, A. M. (2015). Review on the Role of Ports in the Development of a Nation. Aquatic Procedia, 4, 295-301.

Geers, K. (2008). Cyberspace and the Changing Nature of Warfare. SC Magazine, 27.

Green, J. A. (Ed.). (2015). Cyber Warfare: A Multidisciplinary Analysis. Routledge.

Hildreth, S. A. (2001, June). Cyberwarfare. Library of Congress Washington DC Congressional Research Service.

Hørthe, G. (2020, August 25). The Three Pillars of Cyber Security. Retrieved January 16, 2022, from Nemko: https://www.nemko.com/blog/the-three-pillars-of-cyber-security

Johnson, T. A. (Ed.). (2015). Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. CRC Press.

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate. Journal of Strategic Studies, 36(1), 125-133.

Korstanje, M. E. (Ed.). (2016). Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities. IGI Global.

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity. Discover Internet of Things, 1(1), 1-14.
Lieber, K. (2014). The Offense-Defense Balance and Cyber Warfare. Cyber Analogies, 96-104.
Lupovici, A. (2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. Military and Strategic Affairs, 3(3), 49-62.
Nguyen, R. (2013). Navigating Jus Ad Bellum in the Age of Cyber Warfare. Calif. L. Rev., 101, 1079.
Parks, R. C., & Duggan, D. P. (2011). Principles of Cyberwarfare. IEEE Security & Privacy, 9(5), 30-35.
Saltzman, I. (2013). Cyber Posturing and the Offense-Defense Balance. Contemporary Security Policy, 34(1), 40-63.
Sheldon, J. B. (2016, May 25). Cyberwar. Retrieved February 19, 2021, from Encyclopedia Britannica: https://www.britannica.com/topic/cyberwar
Sobers, R. (2020, March 29). Artificial Intelligence vs. Machine Learning in Cybersecurity. Retrieved March 9, 2022, from Varonis: https://www.varonis.com/blog/ai-vs-ml-in-cybersecurity
Streeter, D. C. (2013). The Effect of Human Error on Modern Security Breaches. Strategic Informer: Student Publication of the Strategic Intelligence Society, 1(3), 2.
Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2018, August 1). Cyber Security Challenges in Organisations: A Case Study in Malaysia. 2018 4th International Conference on Computer and Information Sciences (ICCOINS), 1-4.
The Three-Pillar Approach to Cyber Security: Data and Information Protection. (2020). Retrieved January 10, 2022, from DNV: https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683
Valeriano, B., & Maness, R. C. (2018). International Relations Theory and Cyber Security. The Oxford Handbook of International Political Theory, 259.
What Are the 3 Pillars of Cyber Security? (2020, January 15). Retrieved January 16, 2022, from Charter College: https://www.chartercollege.edu/news-hub/what-are-3-pillars-cyber-security