Analyzing Cybersecurity Infrastructure in the United States: Effectiveness of the Current Structure

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Andrew Chau

Fall 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

In the past several years, large scale cyber physical systems have been prone to cyberattacks in which trillions of dollars in damage is done by hackers who target these systems to gain benefits such as money or cryptocurrency by selling personal information obtained or holding systems ransom by shutting them down. Does the United States have a centralized task force or department to deal with these increasingly common and dangerous cyber crimes? The consequences vary due to each unique situation, however, millions of people are usually negatively affected or harmed and the costs for companies are in the millions to billions of dollars. In this paper, I evaluate whether the current cybersecurity infrastructure in the United States is effective based on analyzing the current climate of cyberattacks on cyber physical systems and the infrastructure supporting these systems. This is done by first investigating and researching the current state of cybersecurity infrastructure, cyber attacks, and cyber physical systems both in the United States and worldwide. Then, analyzing how other countries have approached mitigating cyberattacks, such as cyber task forces (European Commission, 2023), versus the United States. Specifically focusing on research done about the European Union's approach to engineering which shines a light on how their cultural and historical factors influence their policy, action, and mindset towards innovation and is a significant backbone in contrasting the United States' approaches which is then applied towards the topic of cyber infrastructure. Next, taking that information to compare and contrast ideas that could be helpful to implement into the current system or infrastructure of cybersecurity in the United States. Lastly, summarizing all insights found from the research and concluding it at the very end. The United States' cultural ideology poses a potential difficulty for legislation to be approved in

mitigating cyber attacks and establishing an updated and effective infrastructure in combating against cyber crime.

Current Climate of Security Infrastructure & Attacks in the Cyber Realm

Cyber Physical Systems Are Vulnerable

It is oftentimes easy to overlook or forget how much technology has been implemented into almost every aspect of our daily lives. In particular, large scale systems (energy, sewage, and water management) have been undergoing transformation to become cyber physical systems since they are increasingly digitized and reliant on technology. A cyber physical system intertwines physical and software components such as implementing sensing, computation, and networking into physical infrastructure. This shift is driven by factors such as efficiency, cost effectiveness, and reliability, which benefits not only companies, but the consumers of these systems. For example, the World Energy Council (2019) states that electric transmission companies depend on automated controls to run their networks and oil and gas companies depend on data networks to track data from their numerous oil and gas wells and thousands of miles of pipelines, management facilities, and interpret operating conditions. No matter which system it is, they all experience improvements due to technological enhancements where each one has unique benefits. In the energy sector, smart grids allow for real-time data collection, optimize power distribution, reduce waste, and enhance grid resilience, which is especially important when we are dependent on electricity to power our smart devices nowadays. In sewage and water management, monitoring water quality, leak detection, and wastewater treatment leads to improved environmental outcomes and sustainability. Furthermore, artificial intelligent algorithms and machine learning are being used to manage these systems more efficiently by predicting and mitigating system failures, optimizing resource allocation, and reducing

maintenance costs. These cyber physical systems are becoming more adaptive with real time monitoring and sustainable through waste detection which benefits both the environment and community.

However, due to these systems becoming more "smart" and digitized, this presents a wide array of new vulnerabilities that can be easily exploited by hackers or people who want to gain something out of disrupting these systems. On May 7, 2021, Colonial Pipeline, the largest fuel pipeline in the United States, suffered from a cyberattack that impacted the computerized equipment responsible for managing the pipeline. It took six days to contain the attack and led to widespread public panic, a fuel shortage due to people frantically buying gasoline, and a spike in gasoline prices. This heavily disrupted the US fuel supply chain since about 45% of all fuel consumed on the East Coast arrives from this pipeline as stated by Kerner (2022). The hacker group responsible for this attack demanded a ransom payment of 75 bitcoin (or about $4.4 million) or they threatened to publicly release sensitive data from the system's servers. On May 9th, President Biden declared a state of emergency for 17 states and Washington D.C. to keep fuel supply lines open. On June 7th, the Department of Justice announced that it had recovered 63.7 of the bitcoins (about $2.3 million) from the ransom payment (Kerner, 2022). Though no people were physically hurt by the pipeline being shut down, it shows a butterfly effect where the economy suffered due to this disruption and the public felt a sense of panic since their resources were being cut off and limited from them. On the flipside, in 2021, a hacker tried to initiate an attack on a Florida water treatment facility where the levels of sodium hydroxide was adjusted from 100 parts per million to 11,100 parts per million (Kardon, 2021). If successful, the attack would have increased the amount of sodium hydroxide to an incredibly dangerous level for people to consume. Something as seemingly small or simple as tweaking the levels of something

in a treatment facility can have truly catastrophic effects on the community where people can suffer from poisoning or even death. These attacks highlight the current state of vulnerability cyber physical systems face where security breaches are too easy and devastating consequences can result.

Current Government Involvement in Cybersecurity

There should be an immediate question of whether there is a government agency in the United States tasked with helping defend against these cyber crimes and whether the Federal Government has gotten more involved in recent years after a steady uptick in attacks? The answer being yes to both, though there may be mixed opinions on whether either is effective in serving the public. As stated by the FBI (2016), the National Cyber Investigative Joint Task Force (NCIJTF) was established in 2008 to address evolving cyber challenges in the United States. It is comprised of over 30 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense with primary responsibilities of coordinating, integrating, and sharing information to support cyber threat investigations. The task force collaborates with international and private sector partners to bring all available resources to use against domestic cyber threats and their perpetrators in efforts to ensure that the privacy rights of all Americans are protected. This agency provides everything that could help solve and mitigate the cyberattacks and crimes in theory, but how much impact do they truly have in these situations? For example, there was no mention of the NCIJTF in the Colonial Pipeline Firmware Attack where only the Justice Department was said to have recovered bitcoin from the ransom demanded. In other regards, The White House (2023) has stated that the Biden Administration has made progress in establishing cybersecurity requirements in key sectors such as oil and natural gas pipelines, aviation, and rail where the Federal Government will use existing

authorities to set necessary cybersecurity requirements in critical sectors. In setting these new cybersecurity requirements, the Biden Administration will work with Congress to develop regulatory frameworks that take into account the resources necessary to implement them. In both these points (out of many) in the National Cybersecurity Strategy plan, there are ideas and goals set in place but no timeline, deadline, or real indication of how it is actually going to be accomplished. Proposed plans take many years to get necessary approvals and resources to make it a reality, however, there is a need for solutions in the present since things move and evolve quickly in the cyber realm.

A Global Issue Plaguing Countries

There might be a misconception that this issue of rising cyberattacks are only plaguing the United States where other countries are "safe" or it does not occur as frequently. In December 2015, there was a power grid hack in Ukraine where around 225,000 people were without power for 1-6 hours due to hackers gaining access to the system's control center through phishing emails with malware (Vijayshankar et al., 2023). This incident occurred during the winter where people can suffer serious injuries or consequences more easily due to a lack of proper heating or hot water and puts into perspective how dangerous a seemingly minor disruption can cause for people. This time it was a couple hundred thousand people (which is still a lot), but next time it could be tens of millions with the ill intent to purposely harm others. By analyzing this one case alone, we can see similarities between the United States and other countries in their struggles against cyberattacks where everyone is equally vulnerable in various fields or systems. Figure 1 below gives a centralized summary of the different cyberattack cases discussed where the diversity of its we can analyze how diverse these attacks were.

Name & Year	Country	Summary

Colonial Pipeline Ransomware Attack (2021)	United States	Hackers accessed the Colonial Pipeline network, stole 100 gigabytes of sensitive data, and infected the network with ransomware which affected many computer systems. As a result, they shut down the pipeline completely leading to widespread public panic of overbuying gasoline.
Florida Water Treatment Plant Cyber Attack (2021)	United States	A hacker briefly adjusted the levels of sodium hydroxide in the water treatment plant and if successful it would be dangerous for people to consume.
Ukraine Power Grid Hack (2015)	Ukraine	Hackers who gained access to a Ukrainian power grid and disrupted the power supply to several regions by remotely manipulating the system's settings. This led to a blackout that lasted for several hours, causing significant disruption to the affected regions.

Figure 1. *Cyberattacks Summarization*- This table summarizes the list of cyberattacks mentioned in the paragraphs above (Created by Author).

All of these attacks are potentially catastrophic and different in their own ways, yet the common consequence is that they all involve hurting people and the community. Where an attack physically occurs does not matter, since its effects are universally felt and the same in any country. Therefore, countries could learn and take notes from one another on how to approach mitigating these attacks and what steps to take to help prevent these situations from reoccurring. For example, the Israel-U.S. Initiative on Cybersecurity Research and Development for Energy, or ICRDE, shows how countries can create better synergy and solutions by working together.

This initiative focuses on researching, developing, evaluating, and demonstrating new technologies to solve challenges facing cybersecurity in energy facilities, where faculty and industry partners (as well as students and postdoctoral researchers) from the United States and Israel collaborate on projects primarily through Zoom (Triolo, 2022). One of the projects involves creating a cyberattack database using data collected from energy grid incident reports and creating algorithms to detect differences between equipment malfunctions and cyberattacks. This shows that rather than competing against one another on who can build better infrastructure or countermeasures against cyber threats, collaboration allows for is possible to triumph against a common enemy.

Looking Elsewhere for Observations

In addition to direct collaboration, there can be a lot to learn from observation alone and in particular focusing on the European Union (EU). As mentioned by Steffensen and Neeley (2017), the EU's regulatory regime is based on the precautionary principle (PP) where they proceed with caution unless there is conclusive evidence that no risk exists or there is a reasonable way to handle the risks. The system gives high priority to non-economic concerns, whereas, the United States' regulatory regime is based on cost-benefit analysis (CBA) which gives priority to economic, quantifiable factors meaning regulation usually happens after conclusive evidence of harm exists. This difference in principle potentially explains why there is a difference in how the United States is approaching developing new cyber strategies versus the European Union where there is more of a sense of urgency in concrete plans and action for the EU since they are more worried about safety and wellbeing versus cost. As discussed by the European Commission (2023), they are planning and developing a Joint Cyber Unit (JCU) which will help civilian, law-enforcement, diplomatic and cyber defense communities cooperate to

prevent, deter, and respond to cyberattacks. They have proposed to build the JCU through 4 gradual steps: assess the organizational aspects and identify EU operational capabilities by 31 December 2021; prepare national incident and crisis response plans and roll out joint preparedness activities by 30 June 2022; operationalise the JCU by mobilizing EU Rapid Reaction teams, following procedures defined in the EU incident and crisis response plan by 31 December 2022; involve private sector partners, users and providers of cybersecurity solutions and services, to increase information sharing and to be able to escalate EU coordinated response to cyber threats by June 2023. This outline detailed with specific deadlines show there is a sense of importance and seriousness in needing to create a centralized team or operational unit in combating against cyber crimes, in comparison to the United States where there has been general outlines but nothing as concrete as such. The United States and European Union are similar where the US has individual states with their own state government, sets of rules and regulations, and laws and the EU has individual countries with their own government, laws, and regulations. However, the EU is able to accomplish an even more difficult task of uniting countries together on developing and deciding on centralized legislation and in this case developing cyber strategies. Therefore, why is the United States having a tough time doing the same? Cyber related attacks have only continued to rise and become more common over the years where the people need legislation and plans that put the community's safety and best interest in mind.

Looking From a Different Lens

Comparing and Contrasting Factors

Building upon this research is the source "Differences in Risk Conception and Differences in Technological Culture" written by Wiebe E. Bijker in 2007. The author uses discourse analysis to show how a similar issue is dealt with differently between two countries

based on deeper factors such as social, cultural, political, or historical background. This is the basis of the research approach for this paper since it is important to explore and investigate the topic from not only the singular lens of the United States. It will allow a deeper dig into underlying factors that previously were not considered in how they affect policy or approach to mitigate cyberattacks.

Post Hurricane Katrina, many high level officials and news networks from the United States went to the Netherlands to gain insight about how to approach mitigating floods and what potential solutions to implement given the long history of floods in the Netherlands. Bijker (2007) states that all parties returned with spirited reports of how the Americans could learn from the Dutch. The source gave historical context of two real life examples of catastrophic floods (one in the United States, one in the Netherlands) in which the conditions in both were extreme and went beyond the expectations / limits of the existing infrastructure and policies in place in regards to flood prevention and response. Millions of people were affected in both situations with thousands of fatalities, many displaced from their homes, and the land itself suffered lots of damage. Both the United States and the Netherlands took measures afterwards to prevent another catastrophic situation from happening with improvement measures on existing flood prevention infrastructure and establishing organizations tasked with handling these disasters. The source's central claim is that when there are different approaches to resolution for a similar issue, one approach is not superior or better than the other. Rather they are different because of factors that have affected the people who are in charge of coming up with these solutions, having different viewpoints on what purpose they want their solution to accomplish. Bijker (2007) argues that the American practice focuses on predicting disasters and mediating the effects once they have happened, in brief: on 'flood hazard mitigation'. Dutch practice is primarily aimed at keeping the

water out. This was based on a differing concept of floods and standard for solutions where it was accepted in the US and followed the “hundred year flood” philosophy (where it is bound to happen), whereas, in the Netherlands the criteria was “1:10,000” where “for a surge level and wave condition occurring with a 1:10,000 probability’. Under these conditions, the defence system should not fail.” (Bijker, 2007). The US accounts that the threshold for these measures will be tested or fail once every hundred years, but for the Netherlands it should only fail in a low probability of 1:10,000 probability.

United States	Netherlands
Flood hazard mitigation	“Keeping the water out”
“Hundred year flood” approach	“1:10,000” probability approach
Neo-liberal, inclination to privatize and individualize public functions	Accepted central role for the national state in all sectors of society
Developed lots of warning systems and evacuation programs post string of hurricanes in the 1950’s. USACE for protection, Weather Service for warning, Federal Emergency Management Agency (FEMA) for insurance.	Established Deltaplan which consisted of the closure of the tidal outlets of the rivers Maas and Rijn and Oosterschelde and built a storm surge barrier for Oosterschelde that remained open under normal circumstances, but could be closed when a storm surge was forecasted.

Figure 2. *United States vs. Netherlands: Flood Mitigation Approaches* - This table summarizes the differences between the United States and Netherlands’ flood mitigation approaches (Created by Author).

The most relevant concept in the source was the cross-cultural comparison between the two countries’ approaches to preventing flood measures from failing since many may be familiar with Hurricane Katrina, but not with the Netherlands’ ”De Ramp”. It adds immense depth to the topic as it shows the scale of the issue being global and not limited to one country. This builds a sense of community showing that many people go through similar hardships at different points of time and place. This draws a parallel back to an aspect of my research where the community universally experiences the same effects from cyberattacks. This enhances the potential of

countries working together to create more productivity and synergy in combating cyberattacks through information sharing and communication due to a “common enemy”. It also talks about the United States’ neo-liberal culture to privatize public functions and can be used as an analysis in my own research how this affects potential policy or lack thereof in response to weak cybersecurity infrastructure. It ties back into the idea of private companies not being held accountable for strict guidelines of what level of cybersecurity infrastructure to have in place when potentially millions of people put blind trust into them.

The author does a solid job of building credibility by showing that they are not biased to either side based on either personal ties to each country or familiarity of knowledge of one situation over the other. This is a similar style of approach in this paper where it is important to acknowledge all sides equally without bias. As shown in figure 3 below, the steps taken for discourse analysis in this research was looking at one source and finding information relevant to the topic, looking at another source (preferably pertaining to another country) that talks about similar information, then finding parallels and differences between the two, and finally synthesizing the findings into the actual research.

1. Look at sources pertaining to the problem or topic
2. Categorize the information found into individual sections
3. Look at another source pertaining to a similar problem as the first (preferably from a different country)
4. Categorize the information found into individual sections
5. Compare and contrast the similarities and differences between the information found between the two
6. Analyze the parallels are dig deeper into factors or cultural differences that affected these similarities or differences
7. Synthesize findings

Figure 3. *Source Analysis Methodology* - This chart shows the methodology of analyzing sources in this STS research (Created by Author).

There is an analytical lens of exploring social, cultural, political, and historical factors to transcend a solely United States focused perspective which helps expand the scope of this paper. The source effectively showed how to implement discourse analysis of underlying factors and cross-cultural comparison into a research topic without being biased to a particular side.

What Is Learned?

Companies Benefit From Cyberattacks

Based on the findings and analysis of the research done in this paper, the United States' heavily economic focused mindset influences the situation heavily where in turn private defense companies can potentially benefit from the lack of an effective government presence in helping to intervene and prevent cyber crimes. Business can be generated for these defense companies where they help vulnerable companies and systems defend from these attacks through upgrading their infrastructure or receiving contracts in cybersecurity. In general, there is a lot of lobbying in the United States across different sectors, therefore, it would not be farfetched to say that these companies have influence over how much the Federal Government should be involved in helping with cybersecurity infrastructure and how influential the NCIJTF is. The Federal Government usually only gets involved when a company is in deep trouble. For example, in the Colonial Pipeline Firmware Attack, President Biden stepped in and declared a state of emergency where the limits on the amount of petroleum products that could be transported within the U.S. mainland were temporarily suspended and shows the severity of the situation. Many of these defense agencies are ranked the best in the world in terms of cybersecurity, so how could something like the Colonial Pipeline Firmware Attack happen so easily when there are resources available to help prevent something like that from happening? Overall, it ties back to the point

from the research mentioned earlier about the United States having a cost-benefit analysis mindset where the defense contract industry is very lucrative and things are not done for free. The culture of private firms coming first in generating profit over public wellbeing is like healthcare in the EU where they have universal health care, whereas, in the US the private healthcare business is untouchable due to its heavy profit. To bring it back, though the majority of these companies who were affected in these attacks were private, there should be a heavier need and emphasis for the government to use resources that are already present to put safety and security of people first.

Analyzing Differences

While it was not shocking, the biggest light bulb that went off while analyzing the cultural differences between the United States and EU was realizing that in almost any field the culture of prioritizing cost-benefit first over almost anything else holds to be true in the field of cybersecurity. This is a multifaceted interaction where one side is not to blame or take responsibility for this culture or system set in place over the course of time. On one side, companies lobby the government to pass legislation that benefits them in some way or influences them towards their perspective and lawmakers can receive their own benefits in exchange for making those requests happen. This is a potential insight into explaining why the European Union can move faster when it comes to approving legislation that has the approval of all countries in the union since certain topics are not politically motivated where the greater good and safety of the people come first. In the United States (in regards to cybersecurity strategies), there are plans or agencies out there to deal with these issues but then the issue of funding, agreement of laws and regulations across all the states, jurisdiction, etc. hinders real change from happening as easily or quickly. Also, the majority of industries in the US are politically

influenced or nuanced in some way and this can affect the goals of companies or agencies where there is an emphasis of accomplishing an agenda over things for the common good.

The Lack of Government Presence

The biggest surprise in this research was that there was already a national cybersecurity task force in the United States, though they were never mentioned or referenced in any of the case studies or articles for the cyberattacks mentioned and researched. This shows how potentially insignificant or rather unknown the task force is and poses the question of whether they are doing their job effectively behind the scenes or if their influence and involvement in mitigating cyber crimes are lacking and needs to be revised. When researching this task force, there was only one page dedicated to it on the FBI's official website and little information on Wikipedia. This does not mean that this an effective way to judge or indicate whether this task force is relevant or serving the public effectively, but it does raise some questions and potential red flags on why no one talks about them.

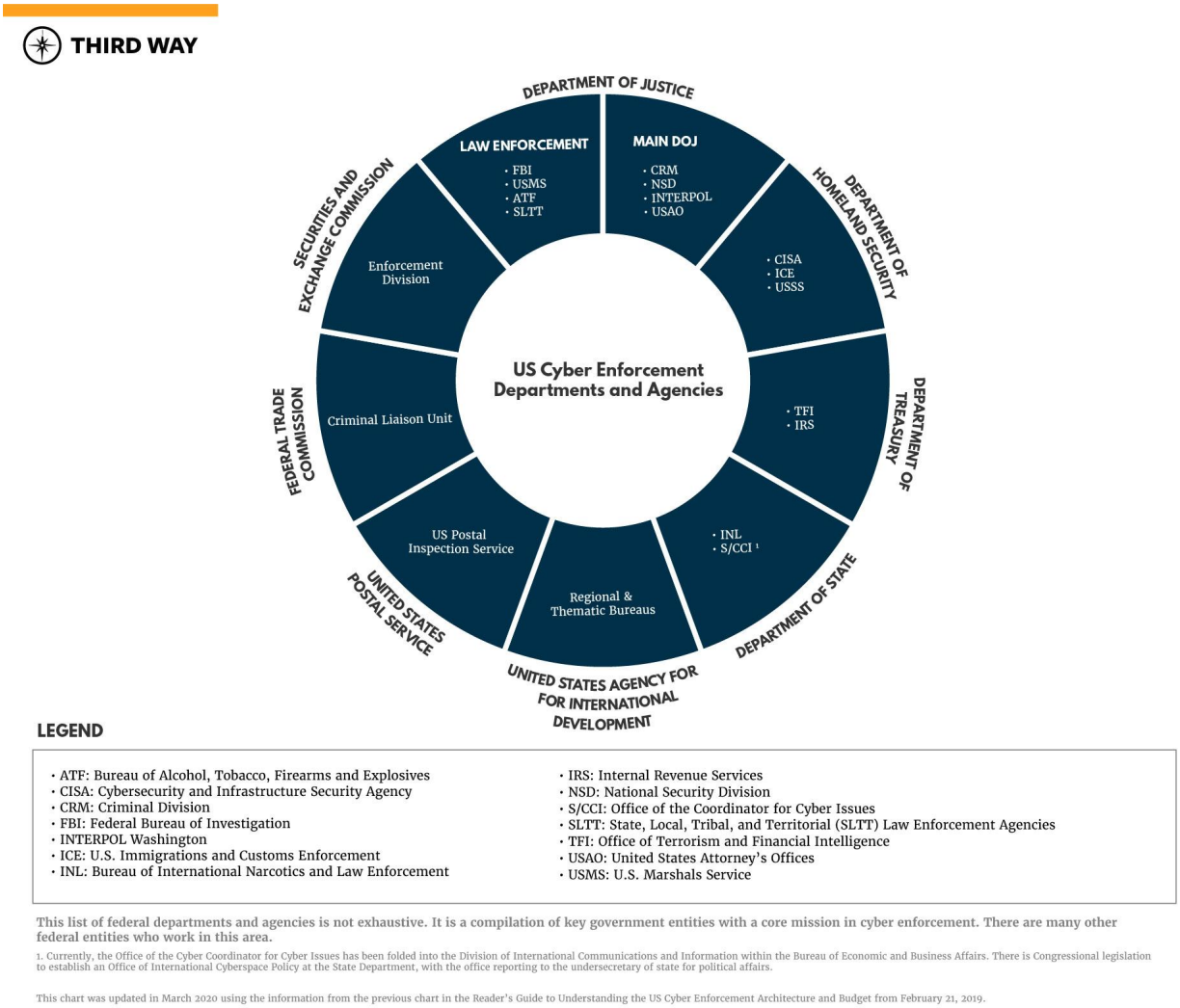

Figure 4. *US Cyber Enforcement Departments and Agencies* - This chart lists all of the agencies in the United States Government responsible for dealing with cyber related activities (Peters & Garcia, 2020).

As seen in figure 4 above, there are many different agencies and organizations dealing with cyber enforcement, however, the NCIJTF is not listed on this chart when it should be center since it is a link between 30 different partnering agencies across law enforcement. The chart could be inaccurate where they forgot to list the NCIJTF, but it shows how the task force is not being seen. This brings up the question of whether the existing task force should be reorganized

or revamped since there should be a strong centralized entity in the middle of this chart as a way for all these agencies to connect in working more efficiently together.

Conclusion

The research from this paper showcases the current climate of the world in terms of cyberattacks that target cyber physical systems and how the United States and European Union have been dealing with it. Discourse analysis for doing cross-cultural comparison in analyzing a similar problem but from two different countries' viewpoints and approach to resolution proved to be helpful in this research where this issue is currently plaguing the world globally. The difference in cultural aspects and mindset between the two is the backbone for explaining the potential contrast in legislation, policy, and urgency in developing new cyber strategies or solutions to combat against these attacks. At the end of this paper, a new viewpoint was brought to the readers about the potential benefits the private sector gains from having loose or rather ineffective systems in place, like the NCIJTF, where they are not prominent nor relevant. This allows for the further questioning of whether private interest and lobbying is influencing the lack of policy or concrete plans for cybersecurity improvements from the United States government. Therefore, the audience is to decide whether the current systems and infrastructure set in place for the United States are effective or if there is more that the government can do to kickstart bigger change and improvement for the field of cybersecurity.

References

Bijker, W. E. (2007). *American and Dutch Coastal Engineering: Differences in Risk Conception and Differences in Technological Culture*. Social Studies of Science, 37(1), 143-151. https://doi.org/10.1177/0306312706069437

European Commision. (2023). *Joint Cyber Unit*. Shaping Europe's digital future. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

FBI. (2016). *National Cyber Investigative Joint Task Force*. FBI. Retrieved from https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

Hong, J. (2023). *How can we make the electric grid more resilient to cyberattacks?* University of Michigan-Dearborn. Retrieved from https://umdearborn.edu/news/how-can-we-make-electric-grid-more-resilient-cyberattacks

Kardon, S. (2021). *Florida Water Treatment Plant hit with Cyber Attack*. Industrial Defender OT/ICS Cybersecurity Blog. Retrieved from https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack

Kerner, S. M. (2022). *Colonial pipeline hack explained: Everything you need to know*. WhatIs.com. Retrieved from https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Peters, A., & Garcia, M. (2020). *A roadmap to strengthen US Cyber Enforcement: Where Do We Go From here?* Third Way. Retrieved from https://www.thirdway.org/report/a-roadmap-to-strengthen-us-cyber-enforcement-where-do-we-go-from-here

Steffensen, B., & Neeley, K. A. (2017), *Precaution and Evidence - Legal Systems as Context Factors of Engineering Innovation and Entrepreneurship.* 2017 ASEE Annual Conference & Exposition. 10.18260/1-2--28752

Sybert, S., Obis, A., Henderson, N., & Whitfield, J. (2023). *Biden's 2024 Budget Impacts IT Modernization Across Government*. GovernmentCIO Media. Retrieved from https://governmentciomedia.com/bidens-2024-budget-impacts-it-modernization-across-government

The White House. (2023). *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*. The White House. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

Triolo, T. (2022). *ASU Researchers Collaborate Internationally to Secure Power Grid.* ASU News. Retrieved from

https://news.asu.edu/20221214-asu-researchers-collaborate-internationally-secure-power-grid

World Energy Council. (2019). *Cyber Challenges to the Energy Transition*. World Energy Council and Marsh & McLennan Companies. Retrieved from https://www.worldenergy.org/assets/downloads/Cyber_Challenges_to_the_Energy_Transition_WEC_MMC_2019.pdf

Vijayshankar, S., Chang, C., Utkarsh, K., Wald, D., Ding, F., Balamurugan, S. P., ... Macwan, R. (2023). *Assessing the impact of cybersecurity attacks on energy systems*. Applied Energy, 345, N.PAG.