**Colonial Pipeline Ransomware Attack**

Stephen Antwi

Old Dominion University

 Interdisciplinary Theory and Concepts

Dr. Kat LaFever

06/18/2023

**Colonial Pipeline Ransomware Attack**

**Abstract**

The Colonial Pipeline Ransomware Attack resulted in the shutdown of about half of the fuel for jets and gasoline supply to the East Coast but a similar attack on the energy infrastructure can be prevented by hardening the security of critical infrastructure, urging countries to perform their responsibilities of deterring criminals from engaging in cyber-crime, and enacting stringent cyber security policies. The dominant justification for cybercrime has been the desire for cybercriminals to realize huge monetary gains. Extant literature has focused on individual disciplinary perspectives on the causes and effects of crime. However, the application of interdisciplinary research can offer a better explanation of the causes and possible ways of preventing cybercrime since it draws from multiple viewpoints. This study uses data from three disciplines to explore the effects of the Colonial Pipeline Ransomware Attack and how similar attacks can be prevented. The interdisciplinary research reveals that different disciplines present varying perspectives on the causes and how cybercrimes can be prevented. Also, interdisciplinary research shows that humans occupy a central position in fighting cybercrime since their actions contribute to this problem.

**Keywords:** *ransomware attack, supervisory control, and data acquisition(SCADA) systems, Industrial Control Systems (ICSs)*

**Introduction**

 The Colonial Pipeline Ransomware Attack is one of the major cyber-attacks in the history of cyber-attacks in the United States. This watershed moment happened on May 7, 2021, when the Colonial Pipeline`s digital system was infected by a ransomware attack. The attack resulted in the shutdown of the pipeline system, affecting airlines and consumers on the East Coast. The research question of this study is: What are the major effects of the colonial pipeline ransomware attack, and what must be done to prevent a similar attack on our energy infrastructure? To better understand the effects of this cyber-attack, and what must be done to prevent a similar attack on our energy infrastructure, different disciplinary perspectives on this issue are considered. This approach is appropriate for this study because the research question is complex since its parts interact in an unanticipated manner. The causes, effects, and what might be done to prevent cyber-attack are not limited to cyber security. In other words, although the research question focuses on cyber security, it draws from other disciplines, such as law and political science. So, a single discipline cannot answer this research question comprehensively. Repko & Szostak (2021) highlights that the “interdisciplinary study is necessitated when the problem or question is multifaceted and functions as a “system” (p.15). Since the problem the research question tries to answer is multifaceted and works as a system, it is essential to follow an interdisciplinary approach to realize a comprehensive understanding.

 Some of the key terms in this paper are *ransomware attacks, SCADA systems,* and *ICSs*. According to Mohurle & Patil (2017), a *ransomware attack* is a software virus that locks the network system, preventing the user from reversing it unless they have the knowledge to do so (p.1938). This virus encrypts the data in the computer in a manner that the user cannot decrypt it without using the decryption key received after paying the ransomware. The *SCADA systems* refer to “underlying monitoring components of many critical infrastructures” (p.1942). These systems offer organizations the tools they need to monitor and control processes in real time. The *ICSs* is “a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures” (Stouffer et al, 2011, p.1).

**History of Colonial Pipeline Ransomware Attack**

 The Colonial Pipeline Ransomware Attack happened in May 2021. During this cyber-attack the attackers gained access to the network system of the Colonial Pipeline via an exposed Virtual Private Network (VPN) account password. The investigations revealed that an employee of Colonial Pipeline had used their password in a different location. The attackers used the password to gain access to the company`s network system. The first intrusion into the system happened on May 6, 2021. On May 7, 2021, the ransomware attack started. The company notified law enforcement agencies about the cyber-attack and decided to take the pipeline network system offline. They also paid 75 bitcoins as ransom to the attackers. The pipeline was restarted on May 12, 2021.

**Relevant Disciplines**

**Cyber Security**

One of the disciplines that offer valuable insights into comprehending the effects of cyber-attacks and how they might be prevented is cyber security. Several researchers have tried to explain cyber-attacks from the cyber security perspective. For example, Gazzan & Sheldon (2023) in their study claimed that the SCADA systems and industrial control systems that control the critical infrastructure contain some features that make them susceptible to ransomware attacks (p.1). The other important concerns these researchers highlighted that lead to cyber-attacks include interoperability, system vulnerabilities, and lack of security awareness and security controls (Gazzan & Sheldon, 2023, p.59). These researchers` observations are influenced by the Routine Activities Theory. This theory postulates that a crime happens when there is a convergence of an inspired criminal, a lack of capable protector, and an appropriate target (Purpura, 2013). So, this theory considers both the criminal and the victim.

An assumption the cyber security viewpoint assumes is that individuals are motivated to engage in cyber-attacks to disrupt regular operations to cause losses. Equally important to note is that this view presents that a cyber-attacker can gain access to the victim`s information system if it lacks adequate security measures. In the case of the Colonial Pipeline cyber-attack the cyber security perspective presents that the attack was caused by the vulnerabilities of SCADA and ICS. These vulnerabilities allowed the hackers to access the network of the Colonial Pipeline, stealing large data and infecting the information system network system with ransomware. This infection affected several computer systems for managing accounting and billing functions. Therefore, according to the cyber security perspective, a similar future cyber-attack can be prevented by hardening the security system of the critical infrastructure. Typically, this encompasses ensuring the SCADA systems have better security systems to prevent cyber-attacks.

**Political Science**

The other discipline that offers helpful insights into understanding the impacts of the Colonial Pipeline Ransomware Attack and how to prevent similar future attacks is political science. This discipline perceives complex problems because of individuals' or groups' pursuit of power (Repko & Szostak, 2021, p.39). Thus, political science views the Colonial Pipeline attack as a cybercrime driven by the exercise of power. It perceives the actors behind the attack as a group of people who wanted to express their power in attacking critical infrastructure. In his study about digital geopolitics, Huskaj (2023) highlighted that “Cyberspace is ubiquitous and affects all domains of human life” (p.153). Huskaj delineates that the Colonial Pipeline attack was caused by the geopolitics between the United States and Russia. According to Huskaj (2023), the DarkSide group, a Russian-based hacking group, was responsible for the attack and it affected many Americans (p.157). It was the first time this pipeline was turned off since 1964. This effect demonstrated the power of the DarkSide to attack the biggest gas pipeline in the United States. In their study, Cavelty & Wenger (2019) observe that digital technologies and negotiation processes are the primary factors that underlie cyber security politics (p.8). Digital technologies relate to how people use these technologies in political settings, while the negotiation processes relate to the "legal boundaries and acceptable rules of behavior"(Cavelty & Wenger, 2019, p.8). Therefore, when people use digital technologies to conduct cyber-attacks this is deemed from a political perspective as a contravention of the legal confines. Cavelty and Wenger`s postulation looks at the political elements of cybercrime. It looks at the nature of politics emerging from the cyber-security event. In this vein, it is pivotal to underscore that after it was discovered that the DarkSide group was responsible for the Colonial Pipeline Ransomware Attack the relations between the United States and Russia deteriorated since the attack was viewed as cyber warfare. The politics surrounding cyber security are shaped by the negotiation processes locally and internationally regarding the duties of each country over the technologies the attackers use. Thus, to prevent future attacks on the energy infrastructure the international negotiations about each country`s responsibility to deter its actors from attacking other nations should be prioritized.

**Law**

The third discipline that offers some useful insights into the causes and effects of the Colonial Pipeline and how a similar attack can be prevented is the law. One of the assumptions this discipline makes about cyber-attacks is that humans act based on existing policies. If the existing policies are weak then the criminals will be motivated to commit crimes. Therefore, from the law perspective cyber-crimes, such as the Colonial Pipeline, can be prevented by applying the concepts of deterrence theory. This theory holds that individuals may obey or contravene a policy by evaluating the consequences and gains of their actions. So, if the consequences exceed the gains the individuals would not engage in crime. From a law perspective, the United States can prevent a cyber-attack by ensuring it enacts stringent policies to deter criminals from engaging in cybercrime. Considering that the malicious actors be based in other nations the United States should partner with other nations in creating and enforcing harsher laws to prevent cyber-crimes. Reeder & Hall (2021) highlighted that to realize long-run success in securing the critical infrastructure in the United States it is essential to have robust and focused leadership that offers clear direction and partners with the other sectors to enhance real-time sharing of information to prevent cyber-attacks (p.20). The policies guiding information sharing of cyber-attacks identified vulnerabilities, coordinated responses, and best practices should be streamlined to prevent cyber-attacks.

Reeder & Hall (2021) argued that the attackers of the Colonial Pipeline exploited the lack of strong safeguards in the system, particularly the lack of a multi-authentication system. This argument reveals that this corporation had not put in place adequate security measures to strengthen its information network system. Therefore, increasing investment in hardening the security of critical infrastructure in the nation can help prevent cyber-attacks on critical infrastructure. Moreover, Kilovaty (2022) argued from a law perspective that the regulations to prevent cyber-attacks should have extra elements besides the existing Transportation Security Administration (TSA) issued guidelines (p.610-611). For instance, this author observes that the TSA policies should include very specific cyber security objectives focusing on addressing cybersecurity (p.611). Cyber security regulations can help prevent cybercrimes by influencing the choices people cyber criminals make.

**Problem Analysis**

The different disciplines offer multiple perspectives on the effects of the Colonial Pipeline attack and how these attacks can be prevented. Drawing from these perspectives it can be argued that multiple factors such as vulnerabilities within this pipeline's network system, geopolitics, lack of stringent laws, and human behavior/interpersonal connections played a role in motivating the attackers to target this critical infrastructure. Thus, different theories such as deterrence theory, rational choice theory, routine activities theory, and theory of space can be used to explain the causes, effects, and how to prevent similar attacks in the future.

**Common Ground**

 This interdisciplinary research shows that there is a common ground among the three disciplines. Political science, law, and cyber security show that the human factor plays a significant role in cyber-attacks. Political science perceives cybercrime because of the quest for power by humans (Repko & Szostak, 2021, p.39). Similarly, the law views cybercrime because of a lack of stringent policies to deter this problem because people act based on the existing rules (Kilovaty, 2022). Likewise, cyber security views cybercrime as a problem stemming from the vulnerabilities inherent in the network system because of the failure of human beings to debug them (Reeder & Hall, 2021). Accordingly, the three theories show that humans play a significant role in cybercrime.

**Conflict between Disciplines**

Although the three disciplines have common ground, they have some conflicts. On the one hand, the cyber security discipline focuses on the vulnerabilities within the critical infrastructure system. For example, Reeder & Hall (2021) argues that the Colonial Pipeline incident was a consequence of a vulnerability in the security system of the company, and they advocated for increasing the defenses of the critical infrastructure (p.15). On the other hand, the political science discipline views the cyber-attack as an effect of geopolitics and the lack of commitment by countries on the global level to prevent their people from engaging in cybercrime (Cavelty & Wenger, 2019, p.8).In contrast, the law disciplinary perspective considers cyber-attacks as a result of a lack of adequate policies. As such, this perspective calls for the enactment of stringent policies to govern the use of cyberspace to deter cybercrimes. Kilovaty (2022) emphasizes that cyber defense responsibilities should be allocated between the public and private sectors (p.651).

**More Comprehensive Understanding**

 Several disciplines provide explanations of the causes and effects of cybercrime as well as how to prevent it. For example, Cyber Security presents an important concept about the relationship between system vulnerabilities and cyber-attacks. This discipline considers the vulnerabilities of the Colonial Pipeline system as the primary cause of the cyber-attack. Integrating this view with the desire of cyber criminals to exploit the vulnerabilities in critical infrastructure reveals why cybercriminals target critical infrastructure. Political science discipline argues that cybercrime can result from geopolitics and the failure of countries to perform their duty of preventing cybercriminals from attacking their targets. In other words, the political science perspective considers cybercrime because of the lack of responsibility of governments at the international level to prevent this crime. The failure of governments to curb cybercrime by fighting this problem locally and partnering with foreign governments offers cybercriminals an opportunity to attack critical infrastructure with vulnerable systems. Therefore, a lack of collaboration among nations contributes to cybercrime. Eventually, the law disciplinary perspective shows that the inadequacy of the existing laws in fighting cybercrime contributes to cybercrime because the malicious actors know that they can evade punishment. Therefore, the three disciplines are interdependent in explaining cybercrime.

**Reflection, Testing, and Communicating the Understanding**

 This interdisciplinary research has proved that using different disciplines in analyzing a complex problem like a cyber-attack can help one arrive at a more comprehensive understanding of the issue. It can also help one to have a better answer to the research question because the different disciplines enable one to examine an issue from multiple viewpoints. However, despite the attempt to develop adequacy in each discipline, my specialization in cyber security is expressed more than other perspectives in the paper. Rather than developing the three disciplinary perspectives equally I inadvertently ended up developing the cyber security perspective more than other perspectives. Also, the limited understanding of the political science perspective on cybercrime hindered me from fully developing insights into this discipline. Applying the Szostak (2009) test to this interdisciplinary research as described by Repko & Szostak (2021) reveals that the paper gives the readers better insights into cyber-crime (p.369). It achieves this by considering various disciplinary perspectives and providing an interdisciplinary perspective on the issue following a multicausal approach. The paper offers a better explanation of the causes and how to prevent cyber-attacks on critical infrastructure.

**Conclusion**

It is abundantly clear that applying the three disciplines to the Colonial Pipeline Ransomware Attack enhances the comprehension of this complex problem`s effects and how similar attacks can be prevented in the future. The four disciplines – cyber security, political science, and law present valuable insights into this attack. Although the underlying theories of the perspectives of these disciplines have some differences, it can be concluded that future cybercrimes can be prevented by countries performing their duty of preventing malicious actors from engaging in cyber-crime, enacting stringent cyber security policies, and enhancing the security of the critical infrastructure.

**References**

Cavelty, M. D., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32. <https://doi.org/10.1080/13523260.2019.1678855>

Gazzan, M., & Sheldon, F. T. (2023). Opportunities for early detection and prediction of ransomware attacks against industrial control systems. *Future Internet*, *15*(4), 144. <https://doi.org/10.3390/fi15040144>

Huskaj, G. (2023). Digital geopolitics: A review of the current state. *International Conference on Cyber Warfare and Security*, *18*(1), 152-161. <https://doi.org/10.34190/iccws.18.1.955>

Kilovaty, I. (2022). Cybersecuring the pipeline. *Hous. L. Rev.*, *60*, 605-651.

Mohurle, S., & Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940.

Purpura, P. (2013). *Security and loss prevention: An introduction*. Butterworth-Heinemann.

Reeder, J., & Hall, T. (2021). Cybersecurity’s Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defense Review*, *6*(3), 15-39. <https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf?ver=6qlw1l02DXt1A_1n5KrL4g%3D%3D>

Repko, A. F., & Szostak, R. (2021). *Interdisciplinary research: Process and theory* (4th ed.). SAGE Publications, Inc.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 1-247.