Nicholas Rossler

Dr. Mohammed Al Kinoon

CYSE 200T

April 25, 2026

Cyber Threats Effecting Critical Infrastructure

Cyber policies and regulations are not able to keep up with the rapid technological change.

In an everchanging and rapidly evolving technological environment, the need to understand cybersecurity and the threats that arise becomes more important. With the rise introducing new cyberthreats the ways to mitigate and understand these attacks are crucial to understanding cybersecurity. In this essay a few topics within cybersecurity will be looked at including common threats, cybercrime and cybersecurity, and critical infrastructure to get a better understanding of cybersecurity. The goal is to look at what these are, and challenges faced when looking at these topics and how they relate to the need to rethink cyber policies in an environment where policies struggle to keep up with rapid changes.

Common threats are common attacks used in the cyber landscape. These are different types of techniques that an attacker may use to get into a system or network. In Module 02D, it contains six of some common threats, these include Advanced Persistent Threats (APTs), Distributed Denial of Service attacks (DDoS), insider attacks, malware, password attacks, and phishing. APTs can be a dangerous attack because of the planning through the process. This shows the attacker targeted a specific target and planned how to get in and grab the data they wanted without being detected. A DDoS attack uses a botnet to send a large amount of traffic to a server to overload it and render their services unusable for a period of time. Insider threats can be dangerous because they are already in the network, they do not have to rely on tools and

techniques that an outside threat would need. Malware is a malicious software that gets introduced to the target, these are dangerous because there are many different forms and as the module points at that others are invented daily. Password attacks are attacks used to get passwords for accounts. They can be done through brute force or dictionary attacks. These attacks can be dangerous if a user uses a simple password that is easy to guess. Phishing attacks are attacks that try to trick a user into giving up their login information. This can be done through a fake email that an attacker sends to trick the user into clicking a link and putting in their login information for the attacker to use.

With so many different ways for an attacker to try and get into a network, knowledge on these attacks and the different strategies to mitigate are important. They can be difficult as they require constant knowledge of the new attacks that keep rising and the many different sectors that can be exploited. In module 04 CS in Cybersecurity, it shows some techniques such as an Intrusion Detection system to help monitor for malicious activities or violations of policies. It can help monitor network traffic inside the network to help catch when malicious activity is being done and stop it before it causes serious harm. Another mitigation tool that can be used is firewalls, these can be used to help stop malicious traffic coming from outside of the network. By using techniques such as packet filtering to filter packets and closing ports to prevent outside traffic from coming into a vulnerable port. Firewalls themselves have limitations as brought up in the modules such as not being able to protect against phishing attacks, as emails are hard to protect against. Another limitation in firewalls is that vulnerabilities may exist within protocols that are allowed through.

Other mitigation techniques are employee training. As employees who are not exposed to the threats of phishing emails are the most susceptible to becoming a victim to them. Making

sure strong password policies are in place helps mitigate risks from password attacks, paired with the use of multi-factor authentication helps strengthen the protection against password attacks. Even if an attacker is to get the password to an account, they now have to get access to an email or mobile device where the code is sent to still get in.

Understanding these different threats and mitigation techniques are important because of rapid technological change. These threats are getting more sophisticated and with more devices getting connected to the internet like the Internet of Things, the attack surfaces are constantly increasing. By understanding these topics, it can help show that security is in a constant battle of keeping up with these common threats.

Cybercrime is a result of these common threats. These common threats can be used by individuals or groups to commit crimes over the internet for a variety of reasons. These reasons may be financial, revenge, political, and even for just recognition. These cybercrimes are important to understand as there are many shortcomings in cybercrime, especially in policies and the way they are governed.

Some of the challenges faced in cybercrime and trying to combat it are anonymity. Bad actors are able to commit crimes on the internet "without revealing themselves and/or their actions to others", making finding the culprit of the crime a hard process (Cybercrime). Bad actors who are more technically skilled know how to use techniques to avoid being identified, making investigating the crime and finding out who was behind it difficult for investigators. Another challenge faced is the borderless nature of the internet. Because cybercrimes may be committed in different parts of the world, the laws and jurisdictions of that place now complicate the process of prosecuting the offender if they are identified. "The lack of harmonized national

cybercrime laws, international standardization of evidentiary requirements" make it hard to investigate cybercrimes and arrest the individual involved (Cybercrime).

What makes cybercrime difficult to regulate is that current policies and regulations in the legal system can't keep up. Because of the rapidly changing environment of technology compared to the slower pace of legislation, cybercrime is harder to prosecute. My understanding of this throughout the semester has shown that the government may need to implement a specialized judicial system for cybercrimes. As this specialized system may be able to focus on cybercrime and be more well informed on technological changes and be able to update policies and frameworks as needed. This can help mitigate the problems faced when dealing with cybercrime in a borderless environment. Another way that can help mitigate cybercrime is global cooperation between nations. This can help combat the shortcomings of investigations that cross different jurisdictions worldwide and help create a framework for cybercrimes committed across the globe.

Cybercrime can target many different individuals and companies, but many may not know that critical infrastructures can also be targeted by cybercrime. Critical Infrastructures include entities such as pipelines, factories, power grids, and water distribution centers and these infrastructures are vulnerable to cyberattacks.

An example of a cyberattack on a critical infrastructure is the Colonial Pipeline ransomware attack in 2021. The Colonial Pipeline attack "created widespread disruption of U.S. fuel supplies along the East Coast" and the damage was bad enough for the President to declare a state of emergency (Cyber Case). This attack was able to happen due to common attacks mentioned earlier, such as weak passwords. The bad actors were able to get into the network "through a compromised VPN password" and the systems also lacked "multifactor

authentication protocols" (Cyber Case). Because of a vulnerable password and the lack of multifactor authentication to help protect against vulnerable passwords, the hackers were able to get into the network and shutdown a critical infrastructure in the United States.

Some mitigation techniques for cyberattacks on critical infrastructure would include not using default passwords and using stronger complex ones. Such as the case with the Colonial Pipeline attack, if they had stronger passwords in play the attack may have possibly been avoided. Another mitigation is the use of multifactor authentication, even with a vulnerable password, multifactor authentication still makes it difficult for bad actors to act off that one password. They now need access to a device or email where the code or a push notification will be sent to accept it and approve the login request. If the Colonial Pipeline had implemented multifactor authentication, they may have been able to protect themselves from an exposed password.

Another mitigation technique is designing critical infrastructures to be more secure. As mentioned in module 05, devices are not designed for security purposes. They are designed to have long lasting life cycles and are inexpensive therefore lacking the technical power to have the protections other devices may have. By developing better cybersecurity policies and installing detection tools within critical infrastructures, these infrastructures can be more closely monitored for abnormal behavior to be investigated.

For the philosophical lens, the need to rethink cyber policy amid rapid technological changes is clear. Throughout the semester it has been shown that technology is rapidly evolving and in cases where the legal system is involved, they are not able to keep up with the evolution of technology. Current policies and regulations also do not keep up, as with critical infrastructures lacking the policies and regulations in place to help mitigate and prevent attacks

on critical infrastructure. Majority of policies and regulations in place focus more on companies and enterprises rather than infrastructures, showing a lack of preparation in that aspect. I think in the future, there needs to be more of a proactive approach towards policies and regulations especially towards critical infrastructures, as attacks on them can lead to wide panic and disruption.

Appendix A

I picked the topics Common Threats, Cybercrime, and Critical Infrastructure because I believed they would transition smoothly with each other. Cybercrime uses a lot of common threats and first clarifying common threats seemed like a good starting point. I chose critical infrastructure because I found it to be overlooked compared to enterprise risks or businesses. As I believe most people believe to look at how cybersecurity can benefit businesses and companies and never think about how it can affect critical infrastructures. For my resources, I used mainly the PowerPoints from the modules mentioned in the writing and listed them again with links in the works cited page. One of the other resources online I used was from Sharing Electronic Resources and Laws on Crime (SHERLOC), as they had a module on cybercrime investigation that provided more insight into challenges investigations may face when it comes to cybercrime. The second resource outside of class PowerPoints I used was from Insurica, also listed in the works cited page, to provide more insight into what happened in the Colonial Pipeline attack. With this resource I was able to provide an example of a critical infrastructure that became a victim due to lack of proper cybersecurity measures in weak passwords and lack of multifactor authentication related to the common threats from topic one. There was no use of AI for this writing.

Works Cited

Al Kinoon, Mohammed. “CYSE-200, Mod 2D Common Threats” CYSE 200. Old Dominion University. https://drive.google.com/file/d/1eDL8k3GcPRKwMxqfiOuHVLIdlwIWwBk0/view Accessed 25 Apr. 2026.

Al Kinoon, Mohammed. “Mod 4: Computer Science’s Contribution to Cybersecurity” CYSE 200. Old Dominion University. https://drive.google.com/file/d/1feuY33nSK5if0dF8z5c9BJcN4aNx1LWr/view Accessed 25 Apr. 2026.

Al Kinoon, Mohammed. “CYSE-200, Mod 5 Cyber Technologies in Engineering Systems” CYSE 200. Old Dominion University. https://drive.google.com/file/d/1TmMfft5Y5wBY0MXEqbcq_0ir4JQWjpiw/view Accessed 25 Apr. 2026.

“Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations.” SHERLOC, www.unodc.org/cld/en/education/tertiary/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html. Accessed 25 Apr. 2026.

Insurica. “Cyber Case Study: Colonial Pipeline Ransomware Attack.” *INSURICA*, 1 May 2025, insurica.com/blog/colonial-pipeline-ransomware-attack/.