Security Council

Cyberattacks on key infrastructure

Research Report

Leiden Model United Nations 2023

"let us sing songs of freedom together"

Forum: Security Council

Issue: Cyberattacks on key infrastructure

Student Officer: Evgeny Ilin

Position: Deputy President

Introduction

Nowadays, every aspect of our world becomes more interconnected and compound than ever before. This is true for countries, people, but also for companies, companies providing our most basic needs for a normal way of life, such as water or electricity.
But the more these organisations, which are essential for our way of life, depend on a network of devices, all working together via the internet, the more they are prone to cyberattacks, targeting these very devices on the internet. Such attacks can have massive consequences for those depending on the resources provided by this critical infrastructure.
The fact that these attacks are carried out via the internet, makes it harder to track and prevent such actions in the future.

This problem needs to be acted upon acutely, in order to minimise the damage inflicted upon civilians.

The issue of "*Cyberattacks on key infrastructure*" is focussing exactly on the following: how to correctly identify and respond to cyberattacks in an appropriate and legal fashion.

Definition of Key Terms

Cyberattack:
"A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorised access to a network, computer system or digital device."[1]

Key infrastructure:
"Critical Infrastructure are those assets, systems, and networks that provide functions necessary for our way of life. This includes systems driving power generation, water treatment, electricity production and other platforms that are interconnected to form the energy grid"[2] [3]

Hacktivist:
"A person who gains unauthorised access to computer files or networks in order to further social or political ends."[4]

Malware:
"Programs written with the intent of being disruptive or damaging to (the user of) a computer or other electronic device; viruses, worms, spyware etc."[5]

Ransomware:
"A type of software that is designed to block access to a computer system until a sum of money is paid."[6]

---

1 https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html, Allianz

2 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience#:~:text=Overview,for%20our%20way%20of%20life., IBM

3 https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html, Allianz

4 https://www.oed.com/search/dictionary/?scope=Entries&q=hacktivist, Oxford English Dictionary

5 https://www.oed.com/search/advanced/Entries?q=malware&sortOption=Frequency, Oxford Reference

6 https://www.oxfordlearnersdictionaries.com/us/definition/english/ransomware#:~:text=%2F%CB%88r%C3%A6ns%C9%99mwer%2F,sum%20of%20money%20is%20paid, Oxford English Dictionary

General Overview

The attackers

In order to get a solid base of understanding of this issue, we first need to look into the people or institutions behind the cyberattacks.
To carry out a big cyberattack, such as the one on Colonial Pipeline in May 2021,[7] there needs to be a team of highly trained hackers, who can crack the software of the company to hinder its normal workflow.
This particular group was called DarkSide. Darkside was interested in ransom, but more on that later.
The important thing now is to recognise that cyberattacks of these scales are nearly never carried out by individuals but by well coordinated groups of hackers.

Attacks performed by just one hacktivist have also taken place in the past, but these are a lot less common. This, however, does not mean they too cannot be dangerous. In February of 2021, a hacker attacked a water plant in Florida, where he increased the percentage of sodium hydroxide in the water to dangerous levels.[8]

One other type of malware developer, the importance of which cannot be understated, are governments. Governments of powerful nations such as Russia and The United States of America often engage in espionage campaigns with the help of cyberattacks on key infrastructure. Not only is spying relevant for these countries, sabotaging countries with opposing views too can be done by cyberattacks. Much resources and money go into development and training of groups of hackers with the very goal to hack into networks of computers, controlling a power plant, or important grid of pipelines.
Examples can be found later in the Research Report.

Motivation

To solve a problem, one needs an understanding of the underlying motivation of those causing the problem.
In this case, the motivations can be sorted in three main categories:

1. Financial Gain
   In the earlier mentioned attack on the Colonial Pipeline[9], the hackers were after profit. They inflicted devices, with which the pipeline was operated, with ransomware. And their winnings from this operation were not little: they received 75 bitcoin, which was equivalent to 4,4 million dollars at the time.
   The attractive thing in all this for the hackers, was that this enormous sum of money could be delivered to them within just several hours after the attack.
   Money, therefore, is one of the biggest motivations for hackers to engage in such cyberattacks.

2. Pushing the Political Agenda

---

7 https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=The%20Colonial%20Pipeline%20hackers%20were,what%20ransomware%20is%20all%20about., Kerner, S. M.

8 https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack#:~:text=On%20Friday%2C%20February%205%2C%202021,days%20before%20the%20Super%20Bowl., Kardon, S.

9 https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=The%20Colonial%20Pipeline%20hackers%20were,what%20ransomware%20is%20all%20about., Kerner, S. M.

Sabotaging a pipeline, or a power station can be a way for hackers to push their political agenda by making themselves the centre of attention. They can influence governmental decisions, by making threats, or they can show the broader public that under a certain regime, key infrastructure is being neglected, and left vulnerable to hacking.

3. Gathering of Intelligence
   By hacking a network of company computers, a hacker has access to much of the - normally confidential - information. This means nations can get an informational advantage over one another by hacking into critical infrastructure networks.
   A group known for espionage on energy stations is Dragonfly, a Russian espionage group.[10]

Dependance on digital networks

The world grows more and more reliant on digital networks. This makes us more vulnerable to cyberattacks, especially if security is not advancing as much, as the new hacking techniques.

Luckily governments are getting more and more aware of these issues and they are innovating, in order to create more safety and stability in our grid of critical infrastructure.

Growing sophistication of cyberattackers

Sadly, the cyberattackers, who still have much to gain from carrying out these attacks on key infrastructure, are growing more sophisticated and clever too. There is a variety of innovative malware programs, which are hard to fight. An example of such a program is Stuxnet, a type of malware first created by the United States and Isreäl to sabotage the nuclear program of Iran.

Stuxnet targeted Programmable Logic Controllers, or PLCs, which are computers built to operate under difficult circumstances, such as heavy shaking. PLCs play a major role in every operation they are used in. By disabling such a computer, the whole operation goes down. Stuxnet was extremely successful and is reported to have destroyed multiple centrifuges in the Iranian nuclear facility.[11]

These types of code are extremely dangerous and are always getting stronger, more difficult to combat, and sometimes even hard to stop. Stuxnet, for example jumped from one PLC to another, travelling via USB-sticks and even getting into other energy-facilities.[12]

---

10 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks, Threat Hunter Team

11 https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html, Trellix

12 https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html, Trellix

Legal discussion

While it is hopefully clear that cyberwarfare is a serious threat to our way of life, what exactly constitutes an act of war is still a grey area. The United Nation has so far not accepted cyberattacks as acts of war. Nor is there a treaty, signed by a sufficient number of countries, proclaiming this.[13]

Until no such treaty is signed, cyberwarfare cannot be considered an act of war. The closest we got to a statement that cyberwarfare is in fact warfare, was in 2007, when many Estonian government websites became the target of Russian cyberattacks, after a conflict about the relocation of a Russian World War II memorial, from one Cemetery to another. NATO had not confirmed, nor denied that this series of attacks on Estonian websites is an actual act of war. [14]

If NATO had been more conclusive on this issue, it would have scared off potential cyberattackers, as they would now be aware, their attack could be considered an act of war. Sadly, no such statement was made, and cyberattacks, to this day, are an underestimated threat if it comes to warfare.
The fact that it might be hard to pinpoint the exact origin of certain attacks, plays a role in the delay of conclusive acting on the international scale. If the attacker is unknown, international law can hardly hold a certain nation responsible.

One might also wonder if a cyberattack can ever be answered by a use of actual force. This remains a philosophical question more than anything else, and deserves an essay of its own to be answered.
A short form answer might go something like this: no matter the manner, in which damage has been done, if the damage suffices a response which could only be carried out through utilising military forces, a state should have the right to respond so, for every state should have the right to protect themselves in an appropriate manner.

The bottom line is that nowadays civilians often suffer from cyberattacks on their infrastructure. There should be clear guidelines as to what exactly constitutes a cyberattack and what responses are acceptable.

Important to note, is that all of the above is only true on a governmental level. A single hacker would not be as greatly influenced if cyberattacks among governments were considered acts of war.
However, if the United Nations came up with clear definitions and guidelines, this could scare individual hacktivists off, as cyberattacks would now be officially considered a threat.

[13] https://www.jstor.org/stable/10.7249/mg877af.18, M. C. Libicki
[14] https://www.jstor.org/stable/10.7249/mg877af.18, M. C. Libicki

Major Parties Involved

United Nations

The United Nations is an organisation, currently made up of 193 member states with the goal to find solutions to common problems that benefit humanity.
As mentioned in the previous section of this document, the United Nations can influence the way governments see cyberwarfare, by establishing a clear definition of what exactly is considered to be cyberwarfare, and making a statement that cyberwarfare can be actual acts of war.

NATO

NATO is a treaty organisation, first created to provide security against the Soviet Union. Nowadays NATO is a major player in geopolitical conflicts and decisions.
Much like the United Nations, NATO can establish their own legislation on cyberwarfare. This will not have the same effect as the UN could have, but it would help bring attention to the problem, and prevent certain future cyberattacks, at least against the member states.

Russia

A big player in the field of cyberattacks is Russia. They are often accused of, and found to be carrying out these attacks against their enemies. Russia has many groups of hackers, set up by the government with the sole purpose to spy on other nations.
It would be wonderful if this behaviour could be restricted, but Russia has shown several times, they do not have much regard for the opinions, sanctions, or threats the West makes.

Timeline of Events

21st of April 2007	Russia carried out a series of devastating cyberattacks on websites of the Estonian government, after a conflict about the relocation of a Russian WWII memorial on Estonian ground. This has shown the power of cyberattacks.
10th of July 2010	Stuxnet, the first virus of its kind, has been detected. It is a very costly and powerful malware, which infected Iran's nuclear operation. It was created by the US and Israël, showing even these governments can engage in such morbid tactics and raising many ethical and legal questions about the nature of cyberattacks.
23rd of December 2015	A Russian group infected the power grids of the Ukrainian Oblasts with malware, causing them both to go down for 1-6 hours. This and the intelligence Russia was able to gather is what made this a key event.
7th of May 2021	The Colonial Pipeline ransomware attack took place. This attack was carried out on an important oil and gasoline pipeline for the Southern United States. It has shown how impactful attacks on critical infrastructure can be.

Possible Solutions

Education

At the end of the day, somewhere in the chain of many cyberattacks, stands a regular employee, downloading a file onto a computer, which is connected to a network of computers, via which the infrastructure is operated. By implementing better education and a culture of awareness toward cyber security, many of these simple mistakes will be prevented.

Protective software

A fairly logical way to prevent future cyberattacks, is to enforce a mandatory instalment of anti-malware, or firewall software. By making this a requirement, much of the dangerous malware can be stopped.

Focus on cybersecurity

Companies should take cybersecurity more seriously. Every company can hire teams of professionals, to minimise the chance of cyberattacks. These teams can create rules, which everybody has to follow, to ensure cybersecurity within the company.

They can also communicate to the management of the company, what could be improved in the IT and cyber sector.

Sources

1. *Cyber attacks on critical infrastructure*. (n.d.). Allianz Commercial. https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html
2. *Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA*. (n.d.). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience#:~:text=Overview,for%20our%20way%20of%20life.
3. *hacktivist - Quick search results | Oxford English Dictionary*. (n.d.). https://www.oed.com/search/dictionary/?scope=Entries&q=hacktivist
4. *malware - Advanced search results in Entries | Oxford English Dictionary*. (n.d.). https://www.oed.com/search/advanced/Entries?q=malware&sortOption=Frequency
5. *ransomware noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com*. (n.d.). https://www.oxfordlearnersdictionaries.com/us/definition/english/ransomware#:~:text=%2F%CB%88r%C3%A6ns%C9%99mwer%2F,sum%20of%20money%20is%20paid
6. *Kerner, S. M. (2022, April 22). Colonial Pipeline hack explained: Everything you need to know. WhatIs.com.* https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know#:~:text=The%20Colonial%20Pipeline%20hackers%20were,what%20ransomware%20is%20all%20about.
7. *Kardon, S. (2021, February 9). Florida water treatment plant hit with cyber attack*. (n.d.). Industrial Defender OT/ICS Cybersecurity Blog. https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack#:~:text=On%20Friday%2C%20February%205%2C%202021,days%20before%20the%20Super%20Bowl.
8. *Threat Hunter Team (*2017, October 20*). Dragonfly: Western energy sector targeted by sophisticated attack group*. Symantec Enterprise Blogs. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
9. *What is Stuxnet? | Trellix*. (n.d.). Trellix. https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html
10. Libicki, M. C. (2009). Cyberdeterrenace and Cyberwar. Appendix A: What constitutes an Act of War in Cyberspace? https://www.jstor.org/stable/10.7249/mg877af.18