Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective

Murdoch Watney
University of Johannesburg, South Africa
mwatney@uj.ac.za

Abstract: Over the years cybersecurity threats to and cyberattacks on the critical infrastructure by state and non-state actors have escalated in intensity and sophistication. Cyberattacks, such as the 2017 NotPetya ransomware attack, the 2020 SolarWinds software supply chain attack and the 2021 Colonial Pipeline ransomware attack, illustrate the vulnerability of critical infrastructure to cyberattacks. Most cyberattacks are committed across borders involving criminal hackers or state supported hackers. Furthermore, critical infrastructure is increasingly interconnected and interdependent. Connectivity brings about the risk of a cyberattack, demonstrated by the 2021 Colonial Pipeline ransomware attack. Interconnectedness also means that the compromise of one critical infrastructure asset can have a domino effect that degrades or disrupts others and results in cascading consequences across the economy and national security. Operational continuity is essential and this may have been one of the reasons why Colonial Pipeline paid a ransom to cyber-attackers. A cyberattack on the critical infrastructure of a state cannot be seen in isolation as the consequences of the attack may impact other states, this was illustrated by the 2017 WannaCry and NotPetya ransomware attacks. The level of sophistication of cyberattacks has increased over the years as shown by the 2020 SolarWinds software supply chain attack. The escalation of attacks has served as a catalyst for governments to address the risk to critical infrastructure. Countries need to have strong government bodies which supervise cybersecurity in their country and work together with their counterparts in other countries by sharing information regarding threats and attacks against critical infrastructure. The discussion focuses on the challenges that threats to and attacks on critical infrastructure present, the possible solutions a government may implement in addressing cyberattacks on critical infrastructure and the accountability of state and non-state actors of cyberattacks on critical infrastructure. The issues are discussed from a legal perspective.

Keywords: critical infrastructure, cybersecurity threats, cyberattacks, ransomware attacks, software supply chain attack, state and non-state cyber-attackers

1. Introduction

Private companies and governments are concerned about the vulnerability of critical infrastructure to the threat of cyberattacks by nation and non-nation-states. An attack on critical infrastructure can have a devasting impact on society's social well-being, health, security, and safety to name but a few.

The first cyberattack against a state took place in 2007 when Estonia became the victim of a Distributed Denial of Service (DDoS) attack committed across borders involving compromised computers from 178 countries (Haatja, 2009). Although the DDoS attack did not cause physical damage or destruction to critical infrastructure as the 2010 Stuxnet, it impacted on the Estonian critical infrastructure where daily operations of various organisations, including banks, government departments and small businesses were seriously impaired (Herzog, 2011; Haatja, 2009).

The discovery of the Stuxnet malware in 2010 — which resulted in a nuclear facility in Iran having its centrifuges damaged via compromised programmable logic controllers (PLCs) — demonstrated that critical infrastructure could be targeted by a cyberattack and cause physical damage or destruction (Cox, 2021). Cox (2021) opines that at the time of the 2010 Stuxnet, critical infrastructure industries used computers designed to ensure operational continuity with little regard for cyber security, because at that stage the threat of a cyberattack on the critical infrastructure may have seemed either low or non-existent. Since then, a number of attacks targeting industrial environments have emerged on the global threat landscape (Cox, 2021).

With the severe and continuing threat that cyberattacks present to critical infrastructure, and the increasing calls to address this threat, the following issues will be discussed from a legal perspective, such as

- The challenges cybersecurity threats to and attacks on critical infrastructure present;
- The possible solutions a government may implement to address cyberattacks on critical infrastructure; and
- The legal position concerning the accountability of state and non-state actors that commit cyberattacks on critical infrastructure.

2. Conceptualising terminology

It is important that terminology relevant to the discussion is conceptualised as it will serve as a point of reference with regards to the discussion of cybersecurity threats to and cyberattacks on critical infrastructure from a legal perspective.

Critical infrastructure is a term used by governments to describe assets, systems and networks - such as communications, data storage or processing, financial services and markets, water and sewerage, energy, healthcare and medical, higher education and research, food and grocery, transport, space technology; and the defence industry sector - whether physical or virtual, which are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (see Rege and Bleiman, 2020). Depending on the country, the definition of what constitutes critical infrastructure varies slightly.

Critical infrastructure components are to a large extent dependant on one another. Communication, information technology, financial, commercial and public services are closely linked, for example, agriculture requires the supply of dam water and water purification and pumps require electricity. Interference with transportation systems may cut off supplies for critical manufacturing and medical supplies. A disruption of a single critical infrastructure can trigger a series of effects, that together can have far worse consequences.

Critical infrastructure is vulnerable to cyberattacks. Haatja (2019) defines cyberattacks as "deliberate computer-enabled actions to alter, disrupt, deceive, degrade or destroy adversary computer systems of networks or the information and/or programs resident in or transiting these systems or networks". Cyberattacks therefore seek to compromise computer security in one or more ways by undermining the integrity of information, undermining the operation of computer systems and/or disrupting the flow of information within a network.

The cyberattacks on critical infrastructure may be committed by criminal (non-state) hackers and state or state-sponsored hackers. Shakarian (2020) draws a distinction between criminal hackers and state or state-sponsored hackers which is relevant when evaluating examples of cyberattacks on critical infrastructure (see par. 3 hereafter). Criminal hackers focus on near-term financial gain as was the case in the Colonial Pipeline ransomware attack (see par. 3 hereafter). Criminal hackers use techniques, such as ransomware, to extort money from their victims, steal financial information and harvest computing resources for activities, including sending spam emails or mining for cryptocurrency. Criminal hackers exploit well-known security vulnerabilities that, had the victims been more thorough in their security, could have been prevented, for example when the hackers used a compromised username and password to breach Colonial Pipeline's network (Turton and Mehrotra, 2021). Criminal hackers typically target organisations with weaker security, such as health care systems, universities and municipal governments. Medical systems tend to use specialty medical devices that run older and vulnerable software that is difficult to upgrade (Shakarian, 2020). On the other hand, hackers associated with national governments have entirely different motives. They look for long-term access to critical infrastructure, gather intelligence and develop the means to disable certain industries. They also steal intellectual property – especially intellectual property that is expensive to develop in fields such as high technology, medicine, defence and agriculture. The amount of effort required to infiltrate one of the SolarWinds victim firms is a telling sign that this was not a mere criminal hack (see par. 3 hereafter).

3. Examples of cyberattacks on critical infrastructure

The following three examples of cyberattacks highlight the changing landscape and growing threats to critical infrastructures.

Example 1: NotPetya ransomware attack

The reason why reference is specifically made to the 2017 NotPetya ransomware attack is that it was described at that time as the most financially damaging cyberattack in history (Haatja, 2019; Shakarian, 2020). It caused billions of US dollars' worth of damage and major disruptions to global shipping and trade.

The NotPetya malware infected computers in a range of government and private organisations in Ukraine and spread to companies and organisations around the world. NotPetya was unique as it disguised itself as a form of ransomware, such as the 2017 WannaCry, but was capable of simultaneously deleting user data (Shakarian,

2020). In 2019, the US disclosed that Russia was responsible for the attack, but Russia denied attribution (see par. 6).

Example 2: 2020 SolarWinds software supply chain attack

SolarWinds, a major software company, was the subject of a cyberattack that spread to its clients, which may have started in 2019 but was only discovered in December 2020. Hackers, believed to be tied to the Russian government, gained access to SolarWinds systems and added a malicious code into the company's software system (Thompson, 2021). The system, called Orion, is widely used by companies to manage IT resources. Orion updates, which included the hacked code, were received by as many as 18000 SolarWinds customers (Mehrotra, 2021). The code created a backdoor to customer's information technology systems, which hackers then used to install even more malware that helped them spy on companies and organisations. The hacking campaign that infected numerous government agencies and tech companies with malicious SolarWinds software had also infected more than a dozen critical infrastructure companies in the electric, oil and manufacturing industries running the same software (Zetter, 2021.) The consequence was the penetration of multiple networks.

SolarWinds is used as an example as it was considered as one of the most devastating cyberattacks in history (Thompson, 2021). It exposed vulnerabilities in global software supply chains that affected government and private sector computer systems and constituted a major breach of national security (Shakarian, 2020). The hack revealed gaps in the US cyber defences and could be the catalyst for rapid, broad change in the cybersecurity industry (Oladimeji and Kerner, 2021; see par. 5; and https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att).

Example 3: 2021 Colonial Pipeline ransomware attack

In May 2021, a ransomware attack was launched on Colonial Pipeline, a private company that controls a significant component of the US energy infrastructure and supplies nearly half of the East Coast's liquid fuels. The FBI attributed the attack to a Russian cybercrime gang (Thompson, 2021; see par. 6).

The Colonial Pipeline ransomware attack illustrates the vulnerability of OT and connectivity. Although the ransomware attack did not directly target the OT – the devices that drive gas flows - but the IT, the consequence of the attack was the shutting down of the OT to prevent the risk of the attack and threatening the safety of the OT. This highlights that threats to both human and environmental safety, along with the uncertainty as to the scope of infection, present as risk factors for sensitive industrial environments (Cox, 2021).

4. Challenges facing the protection of critical infrastructure

The following interlinked challenges are identified:

1) Cybersecurity risk mitigation

The starting point of government and a private company that owns critical infrastructure should be to conduct cybersecurity risk mitigation which involves the use of security policies and processes to reduce the overall risk or impact of a cybersecurity threat. As indicated, NotPetya resulted in billions of US dollars' worth of damage and major disruptions to global shipping and trade which may be the consequence of the risk of a cyberattack not being adequately assessed. In the Colonial Pipeline attack, the OT was shut down to prevent the risk of the attack spreading to the OT (see par. 3). Although the SolarWinds attack appeared to be aimed at the theft of emails and other data, the nature of the intrusions created "back doors" which presents the risk of attacks on physical infrastructure.

Cybersecurity risk mitigation may be separated into four elements: prevention, detection, response and recovery.

With respect to the prevention element: It may be difficult to completely prevent the threat of an attack as protecting all systems from any attacker may not be possible (Hemsley and Fisher, 2018; Thompson, 2021). Hemsley and Fisher (2018) opines that a key lesson learnt from Stuxnet is that a well-financed, sophisticated

threat actor can likely attack any system that it desires. Thompson (2021) opines that preventing ransomware attacks, such as the Colonial Pipeline attack, would require US intelligence and law enforcement to infiltrate every organized cyber-criminal group in Eastern Europe.

Regarding the detection, response and recovery elements: An important take away from the Stuxnet attack (discussed at par. 1) and the subsequent cyberattacks (discussed at par. 3) is the ability to detect, respond and recover from a cyberattack (Hemsley and Fisher, 2018). Where a critical infrastructure has been infiltrated, it should be detected as soon as possible. In this regard, SolarWinds was only detected after some time which impacted negatively on recovery.

2) Interconnectivity and interdependence

Connectivity without proper or insufficient safeguards creates significant vulnerabilities. Tidy (2021) opines that the simplest way to protect OT is to keep it offline with no link to the internet at all. OT networks were traditionally segregated from the Internet in what is known as an 'air gap.' Malware may be installed manually via external media, such as a USB which was used in Stuxnet. Malware external media installation doubled in 2021 with 79% of these holding the potential to disrupt OT. Cox (2021) indicates that the threat of a cyberattack is not completely eliminated in instances where the OT network is segregated.

Over the years operational demands have made critical infrastructure more vulnerable. These include the convergence of IT and OT, the adoption of devices in the Industrial Internet of Things (IIoT), and the deprecation of manual back-up systems (OT). This means that OT can be disrupted by cyberattacks that first target IT systems, rather than having to be installed manually via external media (Cox, 2021).

3) Skill level of threat actors against critical infrastructure and defenders of critical infrastructure

The skill level of sophisticated threat actors is also increasing, as are the frequency of attacks targeting critical infrastructures and the systems that control them. The defenders of these systems need to have equally advanced skills and knowledge to protect essential resources.

4) Outsourcing software

Thompson (2021) opines that SolarWinds did not consider the risk associated with outsourcing software development to Eastern Europe, including a company in Belarus. Russian operatives have been known to use companies in former Soviet satellite countries to insert malware into software supply chains. Russia used this technique in the 2017 NotPetya attack.

5) Investing in cybersecurity of critical infrastructure

Cyber threats are very real, and appropriate investments in cybersecurity should be made by the companies and government.

6) Paying ransom

The issue of paying ransomware is contentious. There are calls that government must prevent ransoms being paid in secret (Tidy, 2021).

The Colonial Pipeline's CEO acknowledged that his company paid a $4.4 million ransom to hackers who were an affiliate of a Russia-linked cybercrime group known as DarkSide, as executives were unsure how badly its systems were breached or how long it would take to restore the pipeline. The hackers also stole nearly 100 gigabytes of data from Colonial Pipeline and threatened to leak it if the ransom was not paid (Turton and Mehrotra, 2021). The latter is an example of extortion ransomware which may be the manner in which these attacks progress in future.

Cox (2021) opines that critical infrastructure— ranging from power grids and pipelines to transportation and health care — must maintain continuous activity. The 2021 ransomware attack against Colonial Pipeline demonstrates why the company paid the ransom as the closure of the pipeline resulted in dangerous panic buys,

long lines at the pump and gas shortages. There was also the issue of extortion being linked to the payment of the ransom.

7) Fragmented approach to cybersecurity of critical infrastructure

Thompson (2021) points out that the fragmentation of the US authorities for national cyber defence evident in the SolarWinds hack is a strategic weakness that complicates cybersecurity for the government and private sector and invites more attacks on the software supply chain.

The official strategy at the time of the 2020 SolarWinds attack is to split cybersecurity responsibilities between the Pentagon for defence and intelligence systems and the Department of Homeland Security (DHS) for civil agencies. Execution of the strategy relies on the Department of Defence's US Cyber Command and DHS's Cyber and Infrastructure Security Agency (CISA). DOD's strategy is to "defend forward", that is, to disrupt malicious cyber activity at its source. CISA, established in 2018, is responsible for providing information about threats to critical infrastructure sectors. Neither agency appears to have sounded a warning or attempted to mitigate the attack on SolarWinds. A private cybersecurity firm called FireEye was the first to notice the breach when it noticed that its own systems were hacked (Jibilian and Canales, 2021). The government's response came only after the attack (see par. 5).

8) Attribution of cybersecurity threats and accountability for cyberattacks

Cybersecurity threats are mostly cross-border and the hacker, either a criminal hacker or state sponsored hacker, will be outside the victim's country borders. In cyberspace, there are no borders at all; hackers in a certain country may well use servers and other digital infrastructure in other countries for their operations (van der Meer, 2020). The SolarWinds attack was launched from inside the US on servers Russian actors had rented from places such as Amazon and GoDaddy, but the actors executed the attack outside the US border. By renting servers in the US, the hackers were able to slip past the National Security Agency (NSA) early warning systems as the NSA is not allowed to conduct surveillance inside the US (see https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att).

Countries such as Russia, Iran and North Korea, are regularly accused of harbouring ransomware groups. For example, federal investigators and cybersecurity agents believe a Russian espionage operation was responsible for the SolarWinds hack (Oladimeji and Kerner, 2021). The Russian government denied any involvement in the attack, releasing a statement that said, "Malicious activities in the information space contradicts the principles of the Russian foreign policy, national interests and understanding of interstate relations." They also added that "Russia does not conduct offensive operations in the cyber domain" (Oladimeji and Kerner, 2021, see par. 6).

There have been calls that state and non-state cyber-attackers on critical infrastructure are held accountable (see par. 6; van der Meer, 2020).

5. Private companies and government response to cybersecurity threats to and attacks on critical infrastructure

The response of the EU, Australia and US are briefly discussed hereafter.

5.1 European Union (EU)

The EU are taking cybersecurity seriously by implementing various initiatives (see https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies).

ENISA ('European Union Agency for Network and Information Security') is the EU agency that deals with cybersecurity. It provide support to member states, EU institutions and businesses in key areas, including the implementation of the NIS Directive. The Cybersecurity Strategy strengthens the role of ENISA. The agency now has a permanent mandate, and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU.

In 2016, the European Commission as part of the EU Cybersecurity Strategy proposed the EU Network and Information Security (NIS) directive. The NIS Directive (see EU 2016/1148) was the first piece of EU-wide cybersecurity legislation. The goal was to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and the national transposition by the EU member states happened in 2018. In 2020, an updated NIS (referred to as NIS2) was introduced (see https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies; https://www.consilium.europa.eu/en/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/) as well as a Directive on the resilience of critical entities. The proposed NIS2 will set the baseline for cybersecurity risk management measures and reporting obligations across all sectors that are covered by the directive, such as energy, transport, health and digital infrastructure. The revised directive aims to remove divergences in cybersecurity requirements and the implementation of cybersecurity measures in different member states. To achieve this, the directive sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each member state. It updates the list of sectors and activities subject to cybersecurity obligations and provides for remedies and sanctions to ensure enforcement. The directive will formally establish the European Cyber Crises Liaison Organisation Network, (EU CyCLONe) which will support the coordinated management of large scale cybersecurity incidents.

The Commission with ENISA is also working on an EU wide certification framework. The Cybersecurity Act outlines the process for achieving this framework.

5.2 Australia

In 2021, the *Security of Critical Infrastructure Act* (SOCIA) *2018* was amended to ensure better protection of critical infrastructure and systems of national significance. The SOCIA provides for a Register of Critical Infrastructure Assets – the register builds a clearer picture of critical infrastructure ownership and control in high-risk sectors, and supports more proactive management of the risks these assets face. Furthermore it imposes mandatory cyber incident reporting – following recent amendments to the SOCI Act, responsible entities for critical infrastructure assets may be required to report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal (https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018

5.3 US government solutions to address critical infrastructure protection

The Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) leads the coordinated national effort with public and private sector critical infrastructure partners to enhance the security and resilience of the nation's critical infrastructure. Following the SolarWinds and Colonial Pipeline attacks, the US government has started various initiatives aimed at improving cybersecurity and addressing the risk to critical infrastructure.

In 2021, the government issued an executive order (available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) which is aimed at modernising the nation's cybersecurity:

- Where a company does business with federal government, the software must comply with certain standards which improves security of software sold to the government.
- IT service providers are required to inform the government about cybersecurity breaches that could impact US networks, and removes certain contractual barriers that might stop providers from flagging breaches.
- Federal government must upgrade to secure cloud services and other cyber infrastructure, and mandates deployment of multifactor authentication and encryption with a specific time period.
- The establishment of a "Cybersecurity Safety Review Board" which comprises public- and private-sector officials, which can convene after cyberattacks to analyse the situation and make recommendations.
- Information-sharing within the federal government by enacting a government-wide endpoint detection and response system.

In 2021, the Cyber and Infrastructure Security Agency (CISA) published the "Rising Ransomware Threat to OT Assets" fact sheet in response to the recent increase in ransomware attacks targeting operational technology

(OT) assets and control systems. The guidance (available at https://www.cisa.gov/publication/ransomware-threat-to-ot):

- provides steps to prepare for, mitigate against, and respond to attacks;
- details how the dependencies between an entity's IT and OT systems can provide a path for attackers; and
- explains how to reduce the risk of severe business degradation if affected by ransomware.

In 2021, the US Department of Energy (DOE) launched an initiative to enhance the cybersecurity of electric utilities' industrial control systems (ICS) and secure the energy sector supply chain. (see https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0).

6. Accountability of state and non-state cyber-attackers

Where a cyberattack has been attributed to a cyber-attacker, the state and non-state actors should be held accountable. Holding cyber-attackers accountable shows that a victim state will not tolerate such activities and involvement, and it may also deter other states from engaging in such cyberattacks (van der Meer, 2020).

Although this is a topic that warrants a discussion on its own, the most important issues relevant to the discussion are highlighted.

6.1 State actors

The US government levelled sanctions against Russia for the SolarWinds attack. The White House indicated that there would be more "seen" and "unseen" responses to the breach. The unseen responses — for example, whether the government is preparing a reprisal attack against Moscow in cyberspace — was not disclosed (see https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/). Whether a reprisal attack for a non-material cyberattack is permissible within the ambit of the international law, is debatable.

Article 2(4) of the United Nations Charter prohibits the use of force in international relations. Whether a cyberattack constitutes as the use of force and amount to warfare within the ambit of the present international law, has been debated (Haatja, 2019). In instances where the cyberattack does not result in material effects such as damage or destruction to a physical object, death or injury to human beings, it would not constitute the use of force within the present international law and is not specifically prohibited by the international law. Haatja (2019) is of the opinion that the present legal position should be reformed. Today society relies on information and communication technology (ICT) and a non-material cyberattack on critical infrastructure has the potential to impact negatively on society. Haatja (2019) opines that the harm caused by non-material cyberattacks should be considered within the scope of Article 2(4) and recognised as a new form of violence that the international law should limit states from engaging in.

6.2 Non-state actors

Van der Meer (2020) indicates that the majority of cyber-attacks in the world are launched by non-state actors, especially criminals looking for money (see par. 2). However, van der Meer (2020) opines that state actors increasingly hire non-state actors to launch more severe cyber-attacks with potentially damaging effects for societies abroad. He indicates that effectively responding to state-launched cyber-attacks is already a complicated task which becomes even more difficult when states hide behind non-state actors.

Van der Meer (2020) discusses a policy brief which explores the problems in dealing with non-state cyber-attackers. He provides the following 7 policy options available to states responding to cyber-attacks which are convincingly attributed to non-state actors:

- Requesting the host state to take action against the attacker;
- If the 'host' state is willing, but is not able to take effective measures against the non-state cyber-attacker, then the requesting state may assist the state in doing so;
- If the 'host' state is doing little or nothing after the request for assistance, while it should be able to do so, a diplomatic protest may be a viable option;

- Employing legal measures, such as an indictment. Indictments will generally occur at a national level, for example under national criminal law;
- Sanctions could also be used to target the non-state actor and/or the state that is not taking effective action against this actor;
- A victim state could also respond to a large-scale cyber-attack by retaliating with a counter- attack; and
- A state could use conventional military retaliation, for example through a proportional strike against a specific location related to the non-state actor behind the cyber- attack or the state from which it operates.

The victim state must consider the risks and benefits of each option before engaging with one of the 7 options.

7. Conclusion

The question today remains how to best achieve robust cyber defence. The different cyberattacks referred to in the discussion demonstrate that the scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

Although a cyberattack cannot be completely eliminated, prevention, detection, response and recovery must be prioritised. An attack must be reported and therefore a mandatory reporting obligation must be considered. There must be a central body assisting with attacks on critical infrastructure. A distinction should not be drawn between a private company owning critical infrastructure or it being operated by government since an attack on critical infrastructure affects national security. The risk of a cyberattack on critical infrastructure owned by a private company cannot be only that company's responsibility, but government must provide support.

Over the years the threat of ransomware attacks has escalated (Rege and Bleiman, 2020). Ransomware attacks have become lucrative because a government body or private company cannot afford to lose data that is locked up and will therefore pay the ransom, especially in instances where it is linked to extortion. The manner in which a country should deal with a non-state or state-sponsored actor who resides in a foreign country presents challenges. An attack on a critical infrastructure should not be held without accountability and here the national and global response should be considered (see par. 6).

Countries need to have strong government bodies that supervise cybersecurity and work together with their counterparts in other countries by sharing information because the protection of critical infrastructure is not only a national security issue, but a global one.

References

Cox, O. (2021) "How cyberattacks take down critical infrastructure", [online] https://www.darktrace.com/en/blog/how-cyber-attacks-take-down-critical-infrastructure/.

Haatja, S. (2019) Cyberattacks and International Law on the Use of Force. Routledge: New York. p. 1 – 10, 52 - 111 – 127, 194, 198.

Hemsley, K.E., and Fisher, R.E. (2018) "History of Industrial Control System Cyber Incidents", [online], https://www.osti.gov/servlets/purl/1505628.

Hertzog, S. (2011) "Revisiting Estonian cyberattacks: digital attacks and multinational response", *Journal of Strategic Security* Vol. 4, No. 2, Strategic Security in the Cyber Age, pp. 49-60, [online], https://www.jstor.org/stable/26463926?seq=10#metadata_info_tab_contents.

Jibilian, I. and Canales, K. (2021) "Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal", [online], https://businessinsider.mx/heres-a-simple-explanation-of-how-the-massive-solarwinds-hack-happened-and-why-its-such-a-big-deal/.

Mehrotra, K. (2021) "SolarWinds hack leaves critical infrastructure in the dark on risks", [online], https://www.bloomberg.com/news/newsletters/2021-01-05/solarwinds-hack-leaves-critical-infrastructure-in-the-dark-on-risks.

Oladmeji, S. and Kerner, SM. (2021) "SolarWinds hack explained: everything you need to know", [online], https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Rege,A., and Bleiman, R. (2020) "Ransomware attacks against critical infrastructure", Proceedings of the 19th European Conference on Cyberwarfare and Security, pp. 324 – 333.

Shakarian, P. (2020) "The Sunburst hack was massive and devastating – 5 observations from a cybersecurity expert", [online], https://theconversation.com/the-sunburst-hack-was-massive-and-devastating-5-observations-from-a-cybersecurity-expert-152444.

Thompson, J. (2021) "The Colonial Pipeline cyberattack and the SolarWinds hack were all but inevitable. Why national cyber defence is a 'wicked' problem", [online], https://www.virginiamercury.com/2021/05/13/the-colonial-pipeline-cyber-attack-and-the-solarwinds-hack-were-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem/.

Turton, W. and Mehrotra, K. (2021) "Hackers breached Colonial pipeline using compromised password", [online], https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Tidy, J. (2021) "Colonial Hack: How did cyber-attackers shut off pipeline", [online], https://www.bbc.com/news/technology-57063636.

Van der Meer, S. (2020) "How states could respond to non-state cyber-attackers", [online], https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf.

Zetter, K. (2020) "Infected critical infrastructure, including power industry", [online], https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure.