# Cyber Warfare and Critical Infrastructure

**Xavier Ramage, Khutso Lebea and Siphesihle Sithungu**
University of Johannesburg, South Africa

221006623@student.uj.ac.za
klebea@uj.ac.za
siphesihles@uj.ac.za

**Abstract:** This paper identifies the growing threat that cyber warfare poses to a country's Critical Infrastructure (CI) and the Critical Information Infrastructure (CII) that accompanies it. CI is a term that describes all of the essential systems and services needed for the nation to function. CII describes the Information Systems responsible for the CI's operation. This includes energy grids, finance, water supplies, transportation, and healthcare facilities. This paper will focus mainly on the CI related to energy grids and finance. With the growing integration of digital technologies into these sectors and their CII, efficiency and connectivity have greatly been improved but have also introduced many vulnerabilities, making CII a prime target for cyberattacks. This paper will thoroughly examine cyber warfare's consequences on a country and its CI using real-world examples to determine its risks. A theoretical approach and the National Institute of Standards and Technology (NIST) framework will be analysed using case studies to identify the methods for detecting and patching vulnerabilities in CII. The analysis findings will be used to underscore the necessity of governments and industry leaders to invest in developing a strategy to protect and safeguard the country's CI and CII against cyber warfare.

**Keywords:** Cyberwarfare, Cyberattack, Framework, Information infrastructure, Detection, Critical infrastructure

## 1. Introduction

With the growing implementation of computer systems into the operation of Critical infrastructure, the threat of these infrastructures being targeted for a cyber-attack is also growing (Izycki and Vianna, 2021). The definition of critical infrastructure varies amongst the different sources. Still, the one that gives the shortest summary states that critical infrastructure is a term used to describe the systems and assets that are seen as so important to a country or society that the destruction or disruption can cause a significant impact on the country's security, health, or safety (Izycki and Vianna, 2021). The term "cyber" pertains to the digital domain encompassing computers, information, data, networks, and communications (Izycki and Vianna, 2021). Cyberwarfare is defined as the act of one nation utilising cyber-attacks to disrupt or damage the cyber infrastructure of another country (Izycki and Vianna, 2021).

The growing dependence on information systems within a nation's critical infrastructure, called Critical Information Infrastructure (CII), introduces new vulnerabilities that emerging threats can exploit (Bhaiyat and Sithungu, 2017). Nations engaged in war may exploit these vulnerabilities as part of a new form of warfare—cyber warfare. This mode of warfare is characterised by its unpredictability, as it often remains undetected until an attack occurs, necessitating prompt and effective responses to unexpected incidents (Izycki and Vianna, 2021), making it the most dangerous form of warfare. The loss of a critical infrastructure (CI) can compromise a nation's security, making it more vulnerable to physical attacks by the opposing nation (Bhaiyat and Sithungu, 2017). Countries need to be able to defend themselves and create a suitable framework for safeguarding the CII.

Ten sectors fall under the critical infrastructure term. These sectors are Information Communication Technologies, Finance, Manufacturing, Food, Healthcare, Energy and Utilities, Water, Transportation, Safety, and Government (Yusufovna, Alisherovich, Choi, Cho, Abdurashidovich, and Kim, 2009). These sectors are interconnected and rely on each other to function (Wilson, 2014). This paper's main focus will be on two sectors, namely Energy and Utilities, as well as finance, as these two sectors form the basis of all other sectors (Yusufovna et al., 2009). None of the other sectors can function without the needed energy and utilities, and all other sectors rely on finance to purchase, sell, or operate effectively. This will be discussed in further detail later in the paper regarding case studies and real-world examples.

The paper will discuss the theoretical approach to defending against cyber-attacks and cyber warfare by analysing the existing model developed by the National Institute of Standards and Technology (NIST), called the NIST Cybersecurity Framework. The analysis will focus on identifying vulnerabilities, implementing safeguards, and responding by using case studies and existing implementations to generate results. The results of this study will emphasise the necessity of investment from governments and industry leaders to advance the development of cyber warfare defence mechanisms. After all the findings have been accumulated, a proposed solution to the cyber warfare problem will be created and discussed.

## 2. Methodology

The research conducted in this paper uses a qualitative analysis wherein case studies and existing frameworks are compared to highlight and study the threats of cyber warfare on CI. This paper studies evidence-based and documented incidents of cyber warfare and malware attacks on CII. The case studies are selected based on their relevance and importance in demonstrating the real-world impact of cyberwarfare on the vital sectors of a country and its CI. The methodology consists of three phases:

- Case Study Review: A literature review of documented cyber attacks impacting critical infrastructure from academic journals to cybersecurity reports to government documents. Each case study will be scrutinized in terms of attack vectors, vulnerabilities exploited, and impact.
- Comparative Framework Analysis: A thorough comparison of the different cybersecurity frameworks, such as NIST CSF, the Lockheed Martin Cyber Kill Chain, and MITRE ATT&CK. It involves the study of the strengths and limitations of all frameworks and their applicability in countering threats posed by cyber warfare.
- Defence Strategy Formation: Using all of the information gathered from the previous two points to develop a merged defense strategy to minimize the negative impact and risks of cyber warfare. This defensive strategy allows countries to implement cyberwarfare defence mechanisms or improve their already implemented mechanisms.

The research conducted in this paper can contribute to academic discussions to evaluate the existing cybersecurity frameworks and recommend improvements that can be made for a country to achieve resilience against emerging threats.

## 3. Critical Infrastructure at Risk

Critical Infrastructure sectors are often connected to other sectors of Critical Infrastructure due to the migration to the cyber world (Wilson, 2014). If one of the CI sectors fails, it will lead to a cascading effect that will lead to all other sectors failing (Yusufovna et al., 2009). The cyber world, also known as cyberspace, is a virtual environment comprising computer networks, telecommunications networks, and information technology infrastructures (Wilson, 2014). This section will expand on the two sectors of CI mentioned above and state the reason for their CII being prime targets for a cyber warfare attack and the impact these attacks will have on a country. These CIs will be analysed using case studies and examining previous attacks. The reason for attacking CII with cyber-attacks in cyber warfare is to cause disruptions to the country's CI and the way that the country operates daily (Yusufovna et al., 2009). Other reasons for cyber attacks fall under different definitions, such as cyber terrorism and hacktivism, all being for financial gain or a political agenda (Yusufovna et al., 2009). For this paper, the focus will be on cyber warfare as the reason for attacks.

### 3.1 Energy and Utilities

This sector of Critical Infrastructure is responsible for providing energy and utilities like electricity, gas, petrol, and oil to the country to be used as fuel in daily operations (Yusufovna et al., 2009). Every other sector of CI requires energy to function and complete its daily operations. If an attack renders this sector inoperative, the entire country and every process keeping the country running will grind to a halt (Yusufovna et al., 2009). This means the country will be vulnerable and open to further attacks, being either further cyber-attacks or a full-out physical war (Bagchi and Bandyopadhyay, 2018), (Zetter, 2016). Previous cyber-attacks on energy grids have given us some insight into the topic. Some of these attacks occurred for monetary gain and political agenda, but the case studies discussed below will highlight the attacks branching from cyber warfare intentions.

#### *3.1.1 Stuxnet worm attack 2010*

The most popular and indicative example of cyber warfare targeting energy CI is the Stuxnet worm attack of 2010. While the attack did not target the power grid directly, it caused some major destruction to the nuclear enrichment program (used for nuclear energy) of Iran (Karnouskos, 2011). This sophisticated worm was used to exploit the weaknesses in the Industrial Control Systems (ICS) that were running the centrifuges inside the nuclear facilities (Langner, 2011). Stuxnet altered the speed and functionality of the centrifuges, which led to their destruction (Langner, 2011). The concerning factor of this worm is that the interfaces and systems used to monitor the centrifuges did not flag any irregularities in the functionality (Langner, 2011). The Stuxnet worm is the first known cyber-attack that caused real-world harm and damage, thus showing the evolution of cyber

threats and attacks. The malware was highly sophisticated and used zero-day vulnerabilities tailored to attack the Siemens ICS, which shows the advanced nature of the attack (Karnouskos, 2011).

Due to the advanced nature of the attack, it is thought to be a state-sponsored attack to disrupt the uranium enrichment program, likely to disrupt the plans of using the enriched uranium in nuclear weapons programs (Langner, 2011). This attack was considered to be a joint operation by nations, including the United States and Israel (Langner, 2011). This attack further shows the capabilities of cyberwarfare for geopolitical purposes. Furthermore, the Stuxnet worm shows the dangers of the adapting techniques used in cyberwarfare and the generalised use of ICS in different sectors, including the energy and utilities sector (Langner, 2011). This attack not only shows the vulnerabilities of ICS but also the widespread consequences that come from this attack, which have to do with national security, economic stability, and public safety (Langner, 2011). The line between digital and physical is continuously becoming blurred as adversaries seek new techniques to use cyber-attacks or cyber warfare to cause real-world physical harm. This attack also served as a wake-up call to all governments and industries across the globe to develop and deploy new and upgraded cyber-defence measures to safeguard their CI (Langner, 2011).

#### *3.1.2 Cyber attack on the Saudi Arabian Energy Sector 2017 (Aramco)*

A very sophisticated cyber-attack targeted the energy sector of Saudi Arabia in 2017 to incapacitate the largest state-owned oil company, Saudi Aramco (Clark, 2017). This attack has been attributed to one nation-state actor, making it one of the biggest cyber-attacks on energy sectors (Cronin, 2018). The operation mainly focused on disrupting the nation's oil production and distribution networks for an extended period (Clark, 2017). The attack was executed using a variant of the Shamoon virus that was used previously to attack Aramco in 2012 (Clark, 2017), (Cronin, 2018).

The 2017 variant of Shamoon was designed specifically to wipe data from the infected systems, making them useless and inoperable, thus leading to the related IT infrastructure becoming incapacitated (Cronin, 2018). The virus quickly spread through Aramco's entire network, targeting thousands of computers causing damage to the ICS used in oil extraction and processing (Clark, 2017). An estimated 30,000 computers were affected, causing major disruptions to the operations of the company's facilities (Cronin, 2018). The attackers also used advanced features to hide their tracks with multiple layers of malware executed on the systems (Cronin, 2018). Shamoon was designed to wipe the infected systems completely. This made the recovery very difficult and time-consuming (Clark, 2017). The damage inflicted on the Systems of Aramco caused widespread uncertainty for the energy sectors in Saudi Arabia and beyond international borders as it threatened to disrupt oil supplies worldwide (Cronin, 2018). While this attack did not directly target the refining and processing infrastructure of the oil, it caused long-lasting economic damage due to the disruptions caused to the communication infrastructure and the systems and operations needed to produce and export oil (Clark, 2017). The attack thus caused multiple production sites to be inoperable, causing delays in global markets. This raised serious concerns about how vulnerable the systems used in energy production are to cyber threats (Clark, 2017).

The attack on Saudi Aramco has been a rude awakening to the present risks and future attacks in the energy sector, particularly in countries that rely on oil and gas production for economic stability (Clark, 2017). It showed how cyber-capabilities have evolved to reach the energy sector, which can lead to more than just operational disruption. The other consequences of this attack are economic instability and geopolitical conflicts (Cronin, 2018). The Saudi Arabian government responded to this attack by developing and implementing stronger cybersecurity measures for all its energy infrastructures and other CI, including enhanced monitoring and threat detection systems (Clark, 2017). This incident highlighted the growing trend of state-sponsored cyber-attacks on CI. This means that cyber warfare is becoming more prevalent in the world, and countries need to be prepared for attacks that may come in the future (Cronin, 2018).

### 3.2 Finance

This sector of Critical Infrastructure is crucial for providing financial services, including banking, investments, and monetary transactions, which are key to the country's economy and daily operations (Yusufovna et al., 2009). Every other sector of CI relies on the financial sector to maintain its daily operations and to function effectively (Yusufovna et al., 2009). A country's economy would collapse if the financial sector were incapacitated, disrupting services and supply chains nationwide. This scenario would leave the country vulnerable to further cyber-attacks or economic warfare, causing widespread instability (Bagchi and Bandyopadhyay, 2018). The previous attacks on this sector have consisted of different attack vectors but still led to new defence mechanisms against each vector it has experienced.

### *3.2.1 The 2016 Bangladesh Bank Heist*

The 2016 Bangladesh Bank heist has not been officially attributed to any nation-state. However, it is still widely suspected that a state-sponsored actor was behind the attack due to the level of sophistication, complexity, and precision involved in the operation (Kshetri, 2017). The SWIFT network, the heart of international financial transactions, was the focus point of the attack. The attackers used the system to make several fake transactions, totalling US$ 1 billion, from which most transactions were flagged before the processing could be completed (Kshetri, 2017). These transactions ended up causing an $81 million loss, with a financial trail flowing through some intermediate accounts located in the Philippines and Sri Lanka (Kshetri, 2017). This attack involved high-level expertise and strategic planning to penetrate and circumvent the security measures that the banking institution implemented. This suggests that a low-level cybercriminal or cyberterrorist did not do the attack but rather a state-sponsored operation to disrupt the country's financial infrastructure (Kshetri, 2017). This can be seen as the start of economic warfare (Kshetri, 2017).

This means that even the most secure financial transaction networks can be attacked with relevantly common success because the networks consist of outdated or poorly secured mechanisms that are implemented (Kshetri, 2017). The attack that penetrated the multiple layers of security found in the SWIFT system shows the weaknesses present in the framework used by the financial system (Kshetri, 2017). Some other aspects that suggest the validity of a state-sponsored attack are advanced technical skills and a deep understanding of international transaction systems and their vulnerabilities. These aspects are not common knowledge and are only known by the banking institutions of a country that is involved in international transactions (Kshetri, 2017). This attack was seemingly used to disrupt the Country of Bangladesh and to cause economic devastation. This attack highlighted how countries can use the international transaction system in a cyber-attack to weaken the country and cause political and economic harm without a physical military attack (Kshetri, 2017). This attack emphasised the need for international cooperation to develop and implement better security measures to secure the global financial infrastructure from cyber-attacks, preventing global economic instability (Kshetri, 2017).

### *3.2.2 The 2017 NotPetya Malware Attack*

The NotPetya malware attack in 2017 is regarded as one of the most disruptive cyber-attacks from a state-owned operation (Greenberg, 2018) . The malware was initially designed to target Ukrainian organisations but quickly became a much larger cyber incident affecting many other countries. This attack highlighted the damages that can be caused when a cyber-attack is aimed at CI, especially in the financial sector (Greenberg, 2018). NotPetya was a highly advanced malware that was first thought to be ransomware, but it was far more destructive (Greenberg, 2018). The core function of NotPetya was to disrupt and incapacitate systems responsible for operating the CI in multiple sectors: energy, government, and finance (Greenberg, 2018). The malware was designed to spread across the network from one device to the next whilst encrypting the data and the systems themselves, making them completely inoperable (Greenberg, 2018).

The malware affected many international companies and organisations after it spread from the intended target, Ukrainian organisations (Greenberg, 2018). The fast-spreading nature of the malware affected some of the biggest players in the financial sector, including companies like Maersk, Merck, and FedEx (Greenberg, 2018). The financial losses were staggering, with Merck reporting more than $870 million in damages (Greenberg, 2018). This attack demonstrated how interconnected and dependent the global financial sectors are between countries. Financial institutions worldwide were devastated by the malware's effect on the international level, with disruptions being sensed in all CI sectors, which caused a major economic impact worldwide (Greenberg, 2018).

The NotPetya malware also demonstrated the vulnerabilities of modern financial systems, being highly dependent on complex, interconnected systems (Greenberg, 2018). In today's globalised economy, a cyber-attack on a single nation's CI can have a far-reaching effect, as seen with the collateral damage of the NotPetya malware spreading across borders and affecting the Ukrainian entities and financial institutions operating worldwide (Greenberg, 2018). This malware attack was one of the first major cases of cyberwarfare and was most likely executed as an affirmation of political power (Greenberg, 2018). This risk of state-sponsored cyber-attacks is on the rise, and the global nature of this attack underlines the importance of developing defence measures to safeguard the country's CI from cyber threats (Greenberg, 2018).

The aftermath of this attack demonstrated the lapses in cybersecurity in the international financial sector. This is due to outdated and complex systems not being secured properly due to a lack of expert knowledge and

resources (Greenberg, 2018). Counties have since been developing and devoting more resources to the defensive strategies needed to secure their CI from cyber threats. The continuous progression of cyber-attacks highlights how cyber warfare can be used more effectively than traditional military warfare to disrupt and weaken another country (Greenberg, 2018).

## 4. Literature Review

Cyber warfare and its consequences to CI have been increasing the interest of research in the academic field and governing bodies. The relevant studies have explored CI and the cyber threats that can be executed on them, oriented towards the increasing sophistication of these cyber threats. Infrastructures connected to networks and the internet emerged as the first target in a cyber-attack, demonstrating that an attack on one sector has cascading effects on other sectors (Wilson 2014). Bhaiyat and Sithungu (2017) researched how cyber war can exploit the weaknesses of CII and argued the need for stronger defense mechanisms.

Case studies of great cyber-attacks are one of the most common themes across all academic research in the field. As one of the leading research cases, Langer (2011) provided an extensive analysis of Stuxnet and how state-sponsored cyber weapons disrupt CI. The NotPetya malware shows how cyber-warfare shifts the global economic balance (Greenberg, 2018). This adds to the evergrowing evidence of the threat landscape, as well as the impact of cyber warfare on the ground. Other studies argue for intelligence-based cybersecurity frameworks with real-time threat detection and response systems (Bagchi and Bandyopadhyay, 2018).

Despite all of the work done so far by researchers to tackle various aspects of cybersecurity problems, implementing defensive mechanisms tends to be based in different national environments. Most of the recent studies seem to focus on a single attack, rather than multi-vector attacks. The implementation and adoption of cybersecurity frameworks such as NIST CSF, CKC, and MITRE ATT&CK are found to be used ineffectively in non-Western nations. The following comparative framework analysis could help fill the void created by this problem.

## 5. Theoretical Analysis: Comparative Study of Cyberwarfare Defence Frameworks

The increasing presence of cyberwarfare and cyberattacks requires countries to develop a robust and adaptable framework to secure the CI and CII from threats. This section provides a theoretical analysis of some of the leading cybersecurity frameworks used as a basis of cyberwarfare defense frameworks, by comparing the core functionalities of the frameworks and highlighting the advantages and disadvantages of each framework.

### 5.1 NIST Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a widely used framework for managing cybersecurity risks (NIST, 2018). This framework was initially designed for CI but has been adopted by other industries and uses. The framework consists of three primary components (NIST, 2018):

- **Framework Core**: The core can be divided into five more functions. The functions are to Identify, Protect, Detect, and Recover. These functions can be further divided to provide details on every cyber defence activity and vulnerability (Mell, Grossman and Sedgewick, 2020). The Identify function involves asset management, understanding the business environment, governance, risk assessment, and supply chain risk management. This lets the country or organisation know exactly what they need to protect (Mell, Grossman and Sedgewick, 2020). The Protect function encompasses all of the safeguards, like access control, awareness training, data security, and maintenance of the defences and safeguards (Mell, Grossman and Sedgewick, 2020). The Detect function's main focus is identifying cybersecurity events by continuous monitoring and anomaly detection (Mell, Grossman and Sedgewick, 2020). The Response function involves incident response planning, communication, and mitigation strategies to reduce the attack's impact (Mell, Grossman and Sedgewick, 2020). The final function, Recover, emphasises resilience by planning and developing recovery processes for the aftermath of an attack and maintaining communication with stakeholders (Mell, Grossman and Sedgewick, 2020). These functions are in a continuous loop to ensure that the proactive and reactive measures are robust.
- **Implementation Tiers**: The tiers range from Partial (Tier 1) to Adaptive (Tier 4). Tier 1 provides limited awareness of cybersecurity risks. Tier 2 provides adequate security and awareness of threats and procedures. Tier 3 provides good risk management with protocols, security measures, and awareness

policies. Tier 4 is the most advanced, providing advanced risk management, real-time threat intelligence, and adaptive cybersecurity practices and tools.

- **Profiles**: This function allows the framework to be customised to fit the unique risks, needs, and threats of the country or business implementing the framework. This helps bridge the gap between the current and the desired cybersecurity measures and states.

The strengths or advantages of this framework lie in the flexibility and scalability that allow the framework to be adapted to organisations of all sizes and countries (Gross, 2021). The risk-based approach is another strength of the NIST CSF (Gross, 2021). This framework focuses on risk management rather than prescriptive controls, allowing the country or organisation to prioritise their cybersecurity efforts (Gross, 2021).

This framework still possesses some limitations. One of the limitations is the Generalisation. The framework's broad scope can pose a challenge when implementing specific controls without having some additional guidelines (Johnson, 2019). Another downfall of this framework is its slow adaptation to threats. The framework might lag in addressing present and emerging threats due to its need to be updated periodically (Johnson, 2019).

### 5.2 Lockheed Martin Cyber Kill Chain (CKC)

The Lockheed Martin CKC framework is a threat-centric approach. This framework was designed to understand and disrupt the progression of a cyberattack. The framework consists of seven stages that represent each stage of the typical cyberattack lifecycle (Lockheed, 2011):

1. Reconnaissance: The adversaries collect information about the target infrastructure, vulnerabilities, and personnel to plan their attack.
2. Weaponisation: Following the first step, the attacker creates a tailored malicious payload like malware or exploits.
3. Delivery: This method gets the exploit or malicious software to the target machine. Many delivery methods include USB drives, phishing emails, or network vulnerabilities.
4. Exploitation: This step is when the exploit or malicious software is launched on the target machine to allow the attacker to access the target system.
5. Installation: The malware or malicious package installs itself on the target machine, often used to create persistent mechanisms like backdoors.
6. Command and Control (C2): The attackers connect to the compromised system to execute commands or download and exfiltrate data.
7. Action and Objectives: The final step is where the attacker achieves their goals. This can be data theft, system disruption or further system exploitation.
8. These seven stages of the cyberattack lifecycle are used in this framework to detect and disrupt the attack at any stage (Lockheed, 2011). For example, early detection in the Reconnaissance stage (e.g. identifying network scans) can help prevent the attack even before it develops (Lockheed, 2011). Another example in the Installation stage, through endpoint protection, can prevent malware from being installed and ensure that the malware cannot be persistent on the system (Lockheed, 2011).

This framework's strengths lie in the focus on the attack lifecycle and the proactive defence it provides (Lockheed, 2011). The CKC provides insight into the methods and processes followed by the attackers. This stops the attack at any stage of the lifecycle (Lockheed, 2011). By identifying the attacks at each phase, the defensive measures can be deployed pre-emptively to stop the attack from progressing (Lockheed, 2011).

This framework still has some limitations (Klosek, 2020). CKC only works with linear attacks and linear progression. The framework might not capture or work with modern, multi-vector attacks (Klosek, 2020). Another limitation of the CKC framework is because of its broad categories (Klosek, 2020). The framework does not have specific controls or guidelines for specific countermeasures or controls (Klosek, 2020).

### 5.3 MITRE ATT&CK Framework

MITRE ATT&CK is a comprehensive framework that provides the country or organisations with a knowledge base of the adversary's tactics, techniques, and procedures (TTP) (MITRE, 2022). Unlike the CKC, focusing on the lifecycle of an attack, this framework works by emphasising the methods used during the different stages of an attack and preventing these stages from occurring (MITRE, 2022):

- **Tactics and Techniques**: Tactics refers to the attackers' objectives during an attack, such as Initial Access, Exfiltration, or Privilege Escalation. Techniques refer to the detailed methods and procedures

followed by the attackers to achieve their goal, for example, Spear Phishing – sending targeted emails to gain access to the system – or Credential Dumping – Extracting the credentials from system memory or system files .

- **Matrices**: ATT&CK organises TTPs into matrices based on the type of environment in which it is executed:
- *Enterprise Matrix: Focused on Windows, macOS, and Linux environments.*
- *Mobile Matrix: Targets mobile-specific threats.*
- *ICS Matrix: Addresses Industrial Control Systems (ICS) and Critical Information Infrastructure (CII) systems.*

This framework allows the country or organisation to detect and map the activity to known techniques and activities, identify vulnerabilities and gaps in the defensive measures, and aid the development of tailored detection and mitigation techniques (MITRE, 2022). An example of this framework is the detection of unusual PowerShell or Terminal activities and the execution of the mitigation and defensive measures to eradicate the intrusion.

The strengths of this framework are its Granularity and its Integration with tools (Harrison, 2021). Granularity means that ATT&CK provides a detailed insight into the methodologies used to attack the system, enabling the organisation or country to map specific threats to specific techniques to defend against the attack (Harrison, 2021). This framework is widely implemented in cybersecurity tools, allowing automated detection and response techniques (Harrison, 2021).

The ATT&CK framework still comes with some limitations (Abo El Rob, Islam, Gondi, and Mansour, 2024). These limitations result from the Complexity of the framework and the Reactive Focus of the framework (Abo El Rob et al., 2024). ATT&CK consists of an abundance of resources and policies. Without sufficient expertise and resources, this can overwhelm a country or organisation (Abo El Rob et al., 2024). This framework can only detect known methods of intrusion. The Reactive focus of this framework does not allow it to detect or react against novel or unknown threats (Abo El Rob et al., 2024).

## 6. Findings and Proposed Solution

Examining existing frameworks and major cyber-attacks provides some insights into the defensive measures required for a country to defend its CI against cyber warfare. This section will provide some insight into the commonalities between the frameworks described in the previous section and the lessons learnt from the previous major cyber-attacks. After the findings have been discussed, a proposed solution for defending against cyber-attacks or cyberwarfare will be described.

### 6.1 Findings of Frameworks and Past Attacks

All reviewed frameworks – NIST, CKC, and ATT&CK – emphasise the need for a structured approach to understanding and mitigating the cybersecurity risks associated with cyberwarfare and CI. Each framework provided a unique perspective on the defensive measures needed:

- NIST: Uses a cyclical approach based on risk management and risk assessments with five core functions (Identify, Protect, Detect, Respond, Recover)
- CKC: This framework uses a linear approach, allowing it to disrupt the attack at any stage of the lifecycle.
- ATT&CK: This framework maps and mitigates threats by knowing how attacks are executed (Tactics, Techniques, and Procedures)

Some commonalities between these frameworks are based on proactive and reactive measures. These frameworks' core functions and commonalities, allowing them to be successful, are continuous monitoring, incident response, and recovery planning. If these core functions are supported by extensive and comprehensive management and procedures, the framework will effectively safeguard the CI of the country or organisation. Each framework provides a unique method of defending against a cyber attack and proves to be useful in different ways. A comparative analysis of the frameworks is provided below:

| Aspect | NIST CSF | Cyber Kill Chain | MITRE ATT&CK |
|---|---|---|---|
| **Focus** | Risk Management | Attack lifecycle | Adversarial TTPs |

| Aspect | NIST CSF | Cyber Kill Chain | MITRE ATT&CK |
|---|---|---|---|
| **Strengths** | Scalable, adaptable, risk-based | Lifecycle approach, proactive | Granular insights, tool integration |
| **Limitations** | Generalised, slow to adapt | Linear progression, broad categories | Complexity, reactive focus |
| **Application** | Policy and compliance | Threat disruption | Threat detection and mapping |

Some gaps were identified in these frameworks. The nature of modern attacks, being multi-vector attacks, can evade linear-focused frameworks like the CKC. The reactive nature of ATT&CK creates a problem with novel or zero-day attacks as it relies on known attack methods and procedures. These new attacks will not be identified and mitigated using this framework. These frameworks are very complex and need extensive professional knowledge and resources, which smaller organisations and countries do not have. This makes it hard for these organisations and countries to implement a robust cyber warfare or cybersecurity framework.

We have learnt several lessons from past attacks. The Stuxnet worm demonstrated cyberweapons' effects on CI and the ICS that run these infrastructures. This led to implementing ICS-specific control measures in frameworks like MITRE ATT&CK. The attack on Saudi Aramco demonstrated the global impact that can come from state-sponsored attacks on CI. This attack's long-lasting effects prompted some changes to frameworks like NIST to include more robust Intrusion Detection Systems (IDS) and recovery processes. The Bank Heist in Bangladesh demonstrated the exploitation of the vulnerabilities in the SWIFT systems. This attack showed how reliant the international transaction system is on other nations, which could lead to a devastating fallout. This prompted better security procedures in financial transactions and anomaly detection systems. The 2017 NotPetya malware attack showed the potentially devastating outcome of state-sponsored attacks against CI. This malware showed how the interconnected systems of CI can lead to attacks affecting multiple sectors of CI and industries. This attack sparked the development of more robust defence mechanisms and upgraded policies in frameworks like NIST and CKC.

### 6.2 Proposed Solution

Countries worldwide need to establish some safeguards against cyber warfare and cyber-attacks.

The following measures are proposed for nations developing their first defensive strategies against cyber threats and enhancing global resilience against cyber warfare.

- Developing a National Cybersecurity Framework (NCSF) can be done by taking some of the major advantages of each framework and creating a combination of a few components. Some of the key components for developing an NCSF are:
- *Risk Assessment: Start with the NIST SCF-inspired "Identify" phase. This will help identify the CI assets that need to be protected and to determine the risk associated with each asset.*
- *Threat Intelligence: Apply the ATT&CK-inspired insight into TTP to allow for specific defensive measures to be developed against known attack methods.*
- *Lifecycle Defence Strategies: Along with NIST's cyclical approach, implement the linear approach of attack lifecycles from the CKC framework to mitigate any attack phase.*
- *Incident Response and Recovery: Developing plans and protocols for responding to an attack, recovering the system after an attack has been mitigated, and upholding stakeholder communication.*
- Leveraging lessons from notable cyber incidents can help develop new defence measures for all countries and organisations. Some important lessons from the major attacks are international collaboration and shared intelligence, ICS-specific security measures implementation, and improving endpoint security to minimise the human error involved with these attacks.
- Capacity Building and Collaboration:
- *As part of the framework, education and training about cybersecurity threats based on real-world scenarios must be implemented. Encourage those working with the CI to enhance their skills in advanced areas like threat identification and mitigation techniques.*
- *A public-private partnership can prove to be beneficial when developing an NSCF. Governments must work with the private sector to receive the resources and expertise needed to develop the framework.*

- Adopting Advanced Technologies can prove to be beneficial when developing an NCSF. Investing in AI and machine learning can assist in the advancements in AI, allowing it to detect anomalies and predict potential future attacks (Bécue, Praça and Gama, 2021). Implementing blockchain solutions for data exchange and transaction processing and validation could improve the security measures of these transactions (Sakho, Jianbiao, Essaf, and Badiss, 2019). A zero-trust architecture can be implemented (ZTA) to ensure continuous verification of system users and processes (Stafford, 2020).
- Establishing International Standards: Work with international organisations like the United Nations (UN) or NATO to develop cybersecurity protocols that can be used across borders. Advocate for agreements on the responsible use of cyber capabilities to minimise the impact that state-sponsored attacks cause.

With the growing sophistication of cyberwarfare, the need for countries to adopt and implement a robust and adaptive cybersecurity framework becomes more pressing. Having learned valuable lessons from attacks like Stuxnet, Saudi Aramco, NotPetya, and the Bangladesh Bank Heist, countries must prioritise CI protection using proactive measures, collaboration, and innovation. By implementing the known frameworks and fixing some drawbacks, a new breed of cyberwarfare defensive measures can be developed and implemented by both small and large countries and organisations.

## 7. Conclusion

As cyber warfare escalates, the risks to critical infrastructure (CI) and critical information infrastructure (CII) grow exponentially. Increased reliance on digital systems in sectors like energy and finance heightens their vulnerability to sophisticated cyber-attacks, threatening national security, economic stability, and public safety. This study highlights the importance of cybersecurity frameworks in mitigating these threats. While NIST, CKC, and ATT&CK each offer unique advantages, integrating key elements from them can enhance cyber defence strategies. Governments and industry leaders must adopt proactive measures, including continuous monitoring, advanced threat detection, and international collaboration.

The evolving nature of cyber threats demands ongoing research, investment, and policy enforcement. Without robust cyberwarfare defence frameworks, nations remain vulnerable to disruptions that could have irreversible economic and societal consequences. Safeguarding CI and CII must be a global priority to ensure long-term security and resilience.

## References

Abo El Rob, M.F., Islam, M.A., Gondi, S. and Mansour, O. (2024) 'The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector', Issues in Information Systems, 25(3).

Bagchi, A. and Bandyopadhyay, T. (2018) 'Role of intelligence inputs in defending against cyber warfare and cyberterrorism', Decision Analysis, 15, pp. 174-193.

Bécue, A., Praça, I. and Gama, J. (2021) 'Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities', Artificial Intelligence Review, 54(5), pp. 3849-3886.

Bhaiyat, H. and Sithungu, S. (2017) 'Cyberwarfare and its effects on critical infrastructure', International Conference on Cyber Warfare and Security, pp. 536-543.

Clark, T. (2017) 'Saudi Aramco Cyber Attack: An Overview of the 2017 Shamoon Malware Attack', Cybersecurity Journal, 12(4), pp. 35-44.

Cronin, C. (2018) 'The Global Impact of Cyber Attacks on Energy Infrastructure: A Focus on Saudi Aramco', International Journal of Energy Security, 16(2), pp. 102-117.

Greenberg, A. (2018) 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', WIRED. Available at: https://www.wired.com/story/notpetya-cyberattack/.

Gross, J. (2021) 'NIST Cybersecurity Framework Implementation Success Stories'. National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework/success-stories.

Harrison, L. (2021) 'Operationalising the MITRE ATT&CK Framework'. AttackIQ Academy. Available at: https://academy-api.attackiq.com/wp-content/uploads/2023/07/Student-Guide-Foundations-of-Operationalizing-MITRE-ATTCK-v13.pdf.

Izycki, E. and Vianna, E.W. (2021) 'Critical infrastructure: A battlefield for cyber warfare?', ICCWS 2021 16th International Conference on Cyber Warfare and Security, pp. 454.

Johnson, A. (2019) 'Challenges in Implementing the NIST Cybersecurity Framework'.

Karnouskos, S., (2011), November. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4490-4494). IEEE.

Klosek, T. (2020) Limitations of the Lockheed Martin Cybersecurity Kill Chain Model (Doctoral dissertation, Utica College).

Kshetri, N. (2017) 'The Bangladesh Bank Heist: Lessons Learned for Banks and Financial Institutions', Journal of Cybersecurity, 3(1), pp. 1–10.

Langner, R. (2011) 'Stuxnet: Dissecting a Cyberwarfare Weapon', IEEE Security & Privacy, 9(3), pp. 49–51. Available at: https://ieeexplore.ieee.org/document/5951174.

Lockheed Martin (2011) 'The Cyber Kill Chain'. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.htm.

Mell, P., Grossman, D. and Sedgewick, A. (2020) 'The NIST Cybersecurity Framework: A Framework for Cybersecurity Risk Management'. National Institute of Standards and Technology.

MITRE Corporation (2022) 'ATT&CK Framework: Tactics and Techniques'.

National Institute of Standards and Technology (2018) 'Framework for Improving Critical Infrastructure Cybersecurity'.

Sakho, S., Jianbiao, Z., Essaf, F. and Badiss, K. (2019) 'Improving banking transactions using blockchain technology', 2019 IEEE 5th International Conference on Computer and Communications (ICCC), pp. 1258-1263.

Stafford, V. (2020) 'Zero trust architecture', NIST Special Publication, 800, p. 207.

The Cyber Kill Chain (2011) 'The Cyber Kill Chain'. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Wilson, C. (2014) 'Cyber threats to critical information infrastructure', Cyberterrorism: Understanding, Assessment, and Response, pp. 123-136. Springer.

Yusufovna, F.S., Alisherovich, F.A., Choi, M., Cho, E.-s., Abdurashidovich, F.T. and Kim, T.-h. (2009) 'Research on critical infrastructures and critical information infrastructures', 2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security, pp. 97-101.

Zetter, K. (2016) 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', WIRED. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.