Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries

Shreyas Kumar[1] and Gourav Nagar[2]
[1]Texas A&M University, College Station, TX, USA
[2]Independent Researcher

Shreyas.kumar@tamu.edu
gouravnagar@ieee.org

Abstract: Cyber warfare poses a substantial threat in today's interconnected world, where digital attacks can transcend physical boundaries and affect targets globally. Technologically less advanced adversaries, such as smaller nations or organizations with limited resources, face unique challenges in defending against sophisticated cyber attacks from more advanced entities. This paper explores the threat landscape for these adversaries and proposes a tailored threat modeling framework to address their specific vulnerabilities and needs. By examining the evolution of cyber warfare, including historical incidents and the increasing sophistication of cyber attacks, the study highlights the limitations of existing threat modeling approaches like the Cyber Kill Chain, MITRE ATT&CK Framework, and SWOT analysis when applied to less advanced adversaries. A comprehensive literature review underscores the gaps in current research, particularly the necessity for frameworks tailored to asymmetric technological capabilities. Employing a mixed methods approach, the research combines qualitative and quantitative data from primary sources, such as interviews with cybersecurity experts, and secondary sources, including existing literature and case studies. The proposed framework focuses on asset identification and classification, vulnerability assessment, threat analysis, and risk assessment. Proactive measures, such as basic cyber hygiene practices, advanced threat detection systems, and collaboration with technologically advanced allies, are recommended alongside reactive measures like incident response planning and disaster recovery. The importance of international cooperation and information sharing is also emphasized. Case studies of cyber incidents involving less advanced adversaries, such as the attacks on Estonia, Georgia, and Ukraine, validate the framework and demonstrate its practical application. The findings indicate that the tailored threat modeling framework effectively addresses the unique challenges faced by less advanced adversaries, enhancing their ability to mitigate risks and improve their cybersecurity posture. This study provides valuable insights and offers a practical framework to bolster defenses against cyber warfare, with future research needed to explore emerging threats and technologies further.

Keywords: Cyber Warfare, Threat Modeling, Vulnerability Assessment, Incident Response, International Cooperation, Cyber Infrastructures,

1. Introduction

1.1 Motivation and Context

Cyber warfare has emerged as a critical battleground in the modern era, characterized by the use of computer networks to disrupt, damage, or control enemy infrastructure. Unlike traditional warfare, cyber warfare can transcend physical boundaries, affecting targets anywhere in the world. This has significant implications for the national security of modern nation-states, whose much of the infrastructure, power grid, banking systems, and defense systems are managed via Cyber systems against adversaries that are less advanced in terms of online infrastructure to target.

1.2 Significance of the Study

This study aims to explore the threat landscape for technologically advanced nations against less advanced adversaries and develop a tailored threat modeling framework that addresses their specific vulnerabilities and needs. By understanding the unique threats these adversaries face, we can propose effective countermeasures and defense strategies to enhance their cybersecurity posture.

1.3 Research Questions

The primary research questions guiding this study are:

1. What unique threats do technologically less advanced entities pose to advanced adversaries?
2. How can advanced adversaries identify and mitigate these threats effectively?

1.4 Contributions

This paper contributes to the field of cybersecurity by identifying unique threats and vulnerabilities faced by technologically advanced adversaries, developing a tailored threat modeling framework for threats posed by less advanced adversaries, and proposing practical defense strategies to enhance cybersecurity.

2. Background and Related Work

2.1 Why this topic is important

Creating a threat model for cyber warfare against a country with minimal or no internet dependence involves understanding and identifying potential threats and vulnerabilities in offline infrastructure and developing strategies to counteract both cyber and hybrid threats. The primary objectives are to protect critical infrastructure, communication systems, and physical security and defense systems from various types of attackers, including state-sponsored hackers, insider threats, physical saboteurs, and proxies. The assets to protect include power plants and energy distribution networks, water treatment and supply facilities, transportation systems, radio and satellite communication networks, military communication channels, weapon systems, command and control centers, and surveillance and reconnaissance systems. Attack vectors in this context extend beyond traditional cyber attacks to include physical attacks, electronic warfare, insider threats, and hybrid tactics that combine cyber and physical operations. Physical attacks might involve the sabotage of infrastructure, interference with security measures, or attacks on supply chains. Electronic warfare could target radio frequencies, disrupt satellite communications, or compromise local networked devices such as SCADA systems. Insider threats might stem from disgruntled employees or those coerced or bribed into sabotaging or stealing sensitive information. Hybrid tactics could spread disinformation or propaganda to cause confusion and panic. Vulnerabilities in this scenario include unprotected critical systems, outdated or poorly maintained equipment, insecure local networks, and human factors such as lack of cybersecurity awareness and insider threats. Mitigation strategies should focus on enhancing physical security, using electronic countermeasures like frequency-hopping spread spectrum for radio communications and encryption for satellite communications, and implementing strict access controls and monitoring to mitigate insider threats. Regular training programs for employees and raising awareness about potential threats and security best practices are also essential. In terms of response and recovery, it is crucial to establish a clear incident response protocol and conduct regular drills and simulations to ensure readiness. Recovery strategies should include backup and redundancy plans for critical systems and quick repair and replacement plans for damaged infrastructure. Coordination and collaboration with international allies and organizations for intelligence sharing and best practices are vital to strengthening defenses against such threats. By focusing on these components, a technically advanced country can develop a comprehensive threat model to effectively defend against cyber warfare tactics targeting offline and minimally networked infrastructure.

2.2 Historical Context

Cyber warfare has evolved significantly over the past few decades, with early instances of cyber attacks dating back to the 1980s. The advent of the internet and digital technologies has transformed the nature of warfare, enabling actors to conduct attacks remotely and anonymously. Notable incidents such as the Morris Worm in 1988, the 2007 cyber attacks on Estonia, and the Stuxnet attack on Iran's nuclear facilities in 2010 highlight the growing sophistication and impact of cyber warfare.

2.3 Definition and Scope

Cyber warfare involves the use of digital attacks to compromise, disrupt, or destroy information systems, networks, and infrastructure. It encompasses a wide range of activities, including espionage, sabotage, and propaganda, conducted by state and non-state actors.

Threat modeling involves five essential features that are crucial for developing an effective security strategy. The first feature is identifying critical assets that need protection, such as data, systems, and infrastructure. This step is fundamental as it helps in understanding what needs to be safeguarded. The second feature is enumerating potential threats, which includes identifying various threat actors like hackers, insider threats, and state-sponsored entities, and considering their possible attack vectors. This helps in anticipating who might attack and how. The third feature is vulnerability analysis, which involves assessing and documenting existing vulnerabilities within the system. This step requires a thorough review of the security posture of the assets to pinpoint weaknesses that could be exploited by threat actors. The fourth feature is risk assessment, which involves evaluating the risks associated with each

identified threat and vulnerability. This includes considering the likelihood of a threat exploiting a vulnerability and the potential impact on the organization. This step helps in prioritizing risks to focus on the most critical areas. The fifth and final feature is developing mitigation strategies to address the identified risks. This involves implementing technical controls such as encryption and firewalls, making process changes like enhancing incident response planning and conducting regular employee training, and updating policies to strengthen the overall security posture. These strategies aim to reduce the vulnerabilities and improve the resilience of the system against potential threats.

2.4 Existing Threat Modeling Approaches

Existing threat modeling approaches include the Cyber Kill Chain, the MITRE ATT&CK Framework, and SWOT analysis. The Cyber Kill Chain, developed by Lockheed Martin, outlines the stages of a cyber attack, from initial reconnaissance to execution, including reconnaissance (gathering information about the target), weaponization (creating the attack tools), delivery (transmitting the weapon to the target), exploitation (triggering the weapon), installation (installing malware on the target system), command and control (establishing a communication channel), and actions on objectives (executing the attack). The MITRE ATT&CK Framework provides a comprehensive catalog of tactics, techniques, and procedures (TTPs) used by cyber adversaries and is widely used for threat intelligence, detection, and response. SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) is a strategic planning tool used to identify internal and external factors that can impact an organization's security posture. In the literature review, previous case studies have highlighted the vulnerabilities and challenges faced by less advanced adversaries in cyber warfare. Notable examples include the cyber attacks on Estonia, Georgia, and Ukraine, which demonstrated the devastating impact of cyber warfare on less advanced nations. Despite the valuable insights provided by existing research, there is a lack of focus on tailored threat modeling approaches for technologically less advanced adversaries. This study aims to address this gap by developing a framework specifically designed for these adversaries.

3. Methodology

Threat modeling involves five essential features that are crucial for developing an effective security strategy. The first feature is identifying critical assets that need protection, such as data, systems, and infrastructure. This step is fundamental as it helps in understanding what needs to be safeguarded. The second feature is enumerating potential threats, which includes identifying various threat actors like hackers, insider threats, and state-sponsored entities, and considering their possible attack vectors. This helps in anticipating who might attack and how. The third feature is vulnerability analysis, which involves assessing and documenting existing vulnerabilities within the system. This step requires a thorough review of the security posture of the assets to pinpoint weaknesses that could be exploited by threat actors. The fourth feature is risk assessment, which involves evaluating the risks associated with each identified threat and vulnerability. This includes considering the likelihood of a threat exploiting a vulnerability and the potential impact on the organization. This step helps prioritize risks and focus on the most critical areas. The fifth and final feature is developing mitigation strategies to address the identified risks. This involves implementing technical controls such as encryption and firewalls, making process changes like enhancing incident response planning and conducting regular employee training, and updating policies to strengthen the overall security posture. These strategies aim to reduce the vulnerabilities and improve the resilience of the system against potential threats.

3.1 Threat Analysis

Technologically less advanced adversaries typically rely on outdated or less sophisticated technologies, which lack the security features and resilience of more advanced systems. Common technologies include legacy operating systems, unpatched software, and limited network infrastructure. These adversaries are often susceptible to a range of vulnerabilities, including weak password policies, unpatched software, limited network segmentation, and inadequate incident response plans.

State-sponsored entities possess significant resources and capabilities to conduct sophisticated cyber attacks with political, economic, or military objectives. Hacktivist groups are motivated by ideological goals, while criminal organizations seek financial gain. Both can exploit the vulnerabilities of less advanced adversaries to achieve their objectives. Common attack vectors include phishing and social engineering, which exploit human vulnerabilities to bypass technological defenses. Malware and ransomware disrupt or gain unauthorized access to systems, while denial-of-service attacks overwhelm targeted systems with traffic to render them unavailable to legitimate users.

3.2 Development of a Threat Model

Identifying critical infrastructure components, such as power grids, water supply systems, communication networks, and financial services, is essential for effective threat modeling. Protecting sensitive information, financial records, and intellectual property from unauthorized access and theft is also crucial. Vulnerability assessment involves identifying technical vulnerabilities and procedural weaknesses that could be exploited by attackers. Developing potential exploit scenarios helps understand how vulnerabilities could be exploited and the potential impact on the organization.

Intelligence gathering involves collecting and analyzing information about potential threats and profiling attackers to anticipate and defend against specific types of attacks. Estimating the likelihood of attack scenarios and assessing the potential consequences helps prioritize resources and defense measures.

3.3 Defense Strategies

Implementing basic cyber hygiene practices, such as regular software updates, strong password policies, and user education, is essential for reducing vulnerabilities. Advanced threat detection systems, including intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) solutions, can help identify and respond to threats in real-time. Developing comprehensive incident response plans and ensuring disaster recovery and business continuity plans are in place ensures critical operations can continue or quickly resume following an attack. Collaboration with technologically advanced allies provides access to resources, expertise, and intelligence. Participating in information sharing networks enhances detection and response capabilities.

3.4 Case Studies and Validation

Analyzing incidents such as the cyber-attacks on Estonia, Georgia, and Ukraine provides valuable insights and validates the framework. These case studies highlight the importance of preparedness, robust incident response plans, and international cooperation in cybersecurity. Applying the framework to real-world scenarios demonstrates its practicality and effectiveness, assessing its ability to mitigate risks, reduce vulnerabilities, and enhance overall cybersecurity.

By following this methodology, we aim to develop a comprehensive threat modeling framework that effectively addresses the unique challenges faced by technologically less advanced adversaries in cyber warfare. This approach provides valuable insights and practical solutions to enhance cybersecurity defenses.

4. Case Studies

4.1 Cyber Attacks on Estonia (2007)

In 2007, Estonia experienced a series of unprecedented cyber attacks that targeted government, banking, media, and other critical infrastructure websites. These attacks, widely believed to have been politically motivated, were launched following a decision to relocate a Soviet-era war memorial in the capital city of Tallinn. The decision sparked significant unrest among the Russian-speaking population and provoked a strong response from Russia (Armin et al. 2008).

The attacks began on April 27, 2007, and lasted for several weeks. The primary method used was Distributed Denial of Service (DDoS) attacks, which overwhelmed targeted websites with massive amounts of traffic, rendering them inaccessible. The attackers employed botnets—networks of compromised computers—to flood the servers of Estonian institutions with traffic, effectively paralyzing their online presence (Rid 2012).

Estonia's government ministries, banks, media outlets, and other key organizations were severely affected. The country’s banking sector faced severe disruptions, with several major banks having to temporarily suspend their online services. Media outlets struggled to deliver news, and government websites were taken offline, impeding communication and administrative functions (Singer and Friedman 2014).

The Estonian cyber attacks were a wake-up call to the international community about the potential for cyber warfare to disrupt national security and economic stability. Estonia's response included strengthening its cyber defenses and increasing international cooperation on cybersecurity issues. The country also advocated for NATO to recognize cyber attacks as a potential trigger for collective defense measures under Article 5 of the NATO Treaty (Geers 2011).

4.2 Cyber Attacks on Georgia (2008)

In August 2008, during its conflict with Russia over the regions of South Ossetia and Abkhazia, Georgia experienced a coordinated wave of cyber attacks. These attacks were designed to coincide with and support Russia's military operations, demonstrating a new dimension of hybrid warfare where cyber and kinetic operations are used in tandem (Healey 2013).

The cyber attacks on Georgia began on July 20, 2008, escalating significantly as the conflict intensified. The attacks primarily involved DDoS attacks and website defacements. Georgian government websites, including those of the president, parliament, and foreign affairs ministry, were taken offline. Additionally, the websites of news organizations and financial institutions were targeted, disrupting communications and information dissemination (Lewis 2010).

One notable aspect of these attacks was the use of botnets and the coordination of various hacker groups, some of which were reportedly linked to Russian state actors. The attackers also used simple but effective methods like DNS poisoning and SQL injection to compromise Georgian websites (Singer and Friedman 2014).

The defacement of government websites included propaganda messages and images aimed at demoralizing the Georgian population and undermining trust in the government. These cyber operations were synchronized with the physical invasion, creating confusion and hampering Georgia's ability to communicate internally and with the international community (Rid 2012).

The 2008 cyber attacks on Georgia highlighted the strategic use of cyber warfare as a force multiplier in traditional conflicts. They underscored the need for nations to integrate cybersecurity into their national defense strategies and highlighted the importance of international cooperation in addressing cyber threats (Healey 2013).

4.3 Cyber Attack on Ukraine's Power Grid (2015)

On December 23, 2015, Ukraine experienced a sophisticated cyber attack that targeted its power grid, resulting in widespread power outages. This incident marked the first known successful cyber attack on a power grid, setting a precedent for the potential impact of cyber warfare on critical infrastructure (Zetter 2014).

The attack was meticulously planned and executed, involving multiple stages. Initially, the attackers used spear-phishing emails to gain access to the IT networks of several Ukrainian energy companies. Once inside, they deployed malware, including the infamous BlackEnergy trojan, to steal credentials and establish remote access to the control systems (Singer 2015).

The attackers used the stolen credentials to remotely access the control systems and systematically shut down substations, causing power outages across the Ivano-Frankivsk region. They also deployed KillDisk malware to wipe data from the systems, hindering recovery efforts. Additionally, the attackers disrupted the companies' call centers, preventing customers from reporting the outages and further complicating the response (Singer 2015).

The cyber attack affected approximately 230,000 people, leaving them without electricity for several hours. The incident demonstrated the vulnerability of critical infrastructure to cyber attacks and the potential for significant societal impact. It also highlighted the increasing sophistication of cyber adversaries, who can integrate technical exploits with strategic objectives to create widespread disruption (Singer 2015).

The 2015 attack on Ukraine's power grid prompted a global reassessment of the security of critical infrastructure. It underscored the importance of robust cybersecurity measures, incident response planning, and international collaboration to defend against such threats. The incident also reinforced the need for continuous monitoring and improvement of cybersecurity practices to protect vital systems from evolving cyber threats (Zetter 2014).

5. Proposed Threat Model

The scenario in which a technologically advanced nation faces a technologically less advanced adversary presents unique challenges and opportunities in the realm of cyber warfare. The advanced nation, relying on sophisticated, interconnected online systems for its critical infrastructure—including weapons systems, power grids, banking, and water supply—is highly vulnerable to cyber-attacks. Conversely, the technologically inferior adversary has minimal critical online infrastructure, providing fewer targets for cyber retaliation. This section proposes a threat model tailored to this asymmetrical situation, focusing on both offensive and defensive strategies.

5.1 Asset Identification and Classification

The first step in developing a robust threat model is to identify and classify critical assets within the advanced nation. These assets typically include weapons systems, which are often integrated with advanced command and control networks, relying heavily on real-time data and communications. This dependency makes them prime targets for cyber attacks aimed at disabling or manipulating military capabilities. The national power grid, being highly interconnected and dependent on SCADA (Supervisory Control and Data Acquisition) systems, is vulnerable to disruptions that can have widespread impacts on national security and civilian life. Financial institutions, which depend on complex IT infrastructure for transactions, records, and communications, can be thrown into chaos by cyber attacks, leading to economic instability and loss of public trust. Similarly, water supply and treatment facilities that use automated systems are susceptible to cyber threats that could result in public health crises and service disruptions. Communication networks are also critical, as they are essential for both civilian and military operations, and their disruption can hinder emergency responses, military operations, and everyday activities.

5.2 Vulnerability Assessment

Identifying potential vulnerabilities in these critical systems is essential for effective threat modeling. Common vulnerabilities include the use of legacy systems, where many critical infrastructures still operate on outdated software and hardware, making them more vulnerable to attacks due to a lack of updates and patches. The high degree of interconnectivity among systems can allow an attacker to move laterally within the network, increasing the potential damage of a breach. Despite advancements, many systems may still lack robust cybersecurity measures such as encryption, multi-factor authentication, and regular security audits. Human factors also play a significant role, as employees' susceptibility to phishing and social engineering attacks remains a major vulnerability. Comprehensive training and awareness programs are crucial to mitigate this risk.

5.3 Threat Analysis

The primary threats to an advanced nation's critical infrastructure from a less technologically advanced adversary include state-sponsored cyber attacks, which are often well-funded and sophisticated, targeting critical infrastructure to disrupt national security and public order. Hacktivist groups, motivated by political or ideological goals, can carry out disruptive attacks on critical systems to achieve their objectives. Criminal organizations may seek financial gain through ransomware, data theft, or other cybercriminal activities, exploiting vulnerabilities for profit. Insider threats also pose significant risks, as disgruntled employees or those coerced by adversaries can provide access to sensitive systems and data.

5.4 Risk Assessment

To effectively manage risks, it is essential to evaluate both the likelihood and impact of potential cyber-attacks. This involves assessing the probability of different types of attacks based on historical data, intelligence reports, and current threat landscapes. Evaluating the potential consequences of successful attacks, including financial losses, operational disruptions, and reputational damage, helps prioritize resources and defense measures. Identifying which assets are most critical and require the highest level of protection is crucial based on their importance to national security and societal function.

5.5 Defense Strategies

Given the asymmetrical nature of the threat, a multi-layered defense strategy is essential, incorporating both proactive and reactive measures. Implementing basic cyber hygiene practices, such as regular software updates, strong password policies, and comprehensive user education, can significantly reduce vulnerabilities. Advanced threat detection systems, including IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), and SIEM (Security Information and Event Management) solutions, can help identify and respond to threats in real-time. Network segmentation can also be effective by segregating critical networks to limit the potential for lateral movement by attackers within the system. Conducting regular red team exercises to simulate attacks and identify weaknesses in security protocols and defenses is another proactive measure.

In terms of reactive measures, developing and regularly updating comprehensive incident response plans is essential. These plans should outline the steps to be taken in the event of a cyber attack, including identification, containment, eradication, and recovery. Ensuring that disaster recovery and business continuity plans are in place and tested regularly is crucial to maintain critical operations during and after an attack. Establishing robust forensic capabilities to analyze cyber incidents, understand attack vectors, and improve future defenses is also important.

Collaboration and information sharing play a vital role in enhancing cybersecurity defenses. Engaging in international cooperation to share threat intelligence, best practices, and resources with allies and partners can provide valuable support. Collaborating with private sector entities to leverage their expertise and resources can also enhance national cybersecurity. Participating in information-sharing networks helps organizations stay informed about emerging threats and vulnerabilities and disseminate critical information quickly during a cyber incident.

5.6 Case Study: Application of the Proposed Threat Model

Consider a scenario where an advanced nation, reliant on its interconnected online systems, faces potential cyber attacks from a less technologically advanced adversary. The adversary aims to exploit vulnerabilities in the advanced nation's critical infrastructure to cause widespread disruption. To implement the proposed threat model, the first step would be to identify and classify critical infrastructure components, focusing on their interconnectedness and potential points of failure. Conducting comprehensive vulnerability assessments to identify weak points in the infrastructure, considering both technical and human factors, is essential. Gathering intelligence on potential adversaries, their capabilities, and likely attack vectors helps profile attackers to understand their motivations and tactics. Evaluating the likelihood and impact of potential attacks allows for prioritizing resources and defense measures accordingly. Implementing a multi-layered defense strategy that combines proactive measures, such as advanced threat detection systems and cyber hygiene practices, with reactive measures, like incident response planning and disaster recovery, is crucial.

6. Discussion

6.1 Key Findings

The study identifies several unique challenges faced by technologically advanced adversaries when targeting countries with minimal or no internet dependence. These challenges include the need to adapt strategies to bypass traditional cyber attack methods, the difficulty of compromising offline or manually controlled systems, and the necessity of integrating physical sabotage with cyber tactics. Additionally, advanced adversaries must contend with robust physical security measures and the potential for limited intelligence on local infrastructures. This complexity requires a more nuanced approach, combining electronic warfare, insider recruitment, and hybrid tactics to breach and disrupt critical offline systems effectively. The proposed threat modeling framework is shown to be effective in addressing these challenges by providing a structured approach to identifying and mitigating threats. The framework's focus on asset identification, vulnerability assessment, threat analysis, and risk assessment helps less advanced adversaries develop targeted defense strategies.

6.2 Implications for Policy and Practice

Policymakers should prioritize cybersecurity as a critical component of national security and allocate resources accordingly. This includes funding for cybersecurity initiatives, support for international cooperation, and the development of policies and regulations to enhance cybersecurity. Cybersecurity professionals should adopt best practices, such as regular software updates, strong password policies, user education, and the implementation of advanced threat detection systems. Collaboration with other organizations and participation in information-sharing networks are also essential for staying informed about emerging threats and best practices.

6.3 Future Work: Evaluation of Effectiveness

The effectiveness of the threat model can be assessed by monitoring the number of detected and prevented attacks, the speed and effectiveness of incident response, and the resilience of critical systems. Continuous improvement of the threat model is essential, incorporating lessons learned from real-world incidents and advancements in cybersecurity technologies.

The proposed threat model provides a comprehensive framework for defending technologically advanced nations against cyber threats from less advanced adversaries. By focusing on asset identification, vulnerability assessment, threat analysis, and risk assessment, the model helps develop effective defense strategies tailored to the unique challenges of this asymmetrical conflict. Continuous adaptation and improvement of the model, coupled with international cooperation and information sharing, are crucial for maintaining robust cybersecurity defenses in an increasingly interconnected and hostile digital landscape.

7. Conclusion

This study comprehensively analyzes the threat landscape for technologically less advanced adversaries and proposes a tailored threat modeling framework to address their unique vulnerabilities and needs. The framework's focus on asset identification, vulnerability assessment, threat analysis, and risk assessment helps these adversaries develop effective defense strategies. Future research should explore the evolving threat landscape and emerging technologies that may impact cyber warfare. Areas for further study include the use of artificial intelligence and machine learning in cyber defense, the impact of new technologies such as 5G and the Internet of Things (IoT), and the development of international norms and agreements for cyber warfare. This continued exploration will be crucial in adapting and enhancing cybersecurity strategies to protect against increasingly sophisticated cyber threats effectively.

References

Armin, A., Armin, D. and Uzeve, B. (2008) 'Analyzing the 2007 cyber attacks on Estonia', International Journal of Computer Science and Network Security, 8(4), pp. 1-8.

Clarke, R.A. and Knake, R.K. (2010) Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins.

Denning, D.E. (1999) Information Warfare and Security. Reading, MA: Addison-Wesley.

Fidler, D.P. (2013) 'Cybersecurity and Privacy Issues in a Post-Snowden World', Indiana Journal of Global Legal Studies, 20(2), pp. 439-463.

Geers, K. (2011) Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence.

Goldman, J. (2017) 'The Growing Threat of Ransomware', Network Security, 2017(8), pp. 5-8.

Hanson, J.A. and Ulin, R.B. (2013) 'Critical Infrastructure Cybersecurity: Government and Private Sector Efforts to Protect the Nation's Information Technology and Communications', American Journal of Law & Medicine, 39(2-3), pp. 213-241.

Healey, J. (Ed.) (2013) A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Arlington, VA: Cyber Conflict Studies Association.

Jensen, E.T. (2012) 'The Tallinn Manual on the International Law Applicable to Cyber Warfare', American Society of International Law, 106, pp. 377-381.

Kello, L. (2013) 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', International Security, 38(2), pp. 7-40.

Kumar, N. (2024) Threat Modeling for Cyber Warfare Against Technologically Less Advanced Adversary.

Lewis, J.A. (2010) 'The Cyber War Has Not Begun', Center for Strategic and International Studies (CSIS). Available at: https://csis.org/publication/cyber-war-has-not-begun (Accessed: 14 May 2024).

Lockheed Martin (n.d.) 'Cyber Kill Chain'. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Accessed: 14 March 2024).

MITRE Corporation (n.d.) 'MITRE ATT&CK Framework'. Available at: https://attack.mitre.org/ (Accessed: 14 May 2024).

Mueller, M.L. (2010) Networks and States: The Global Politics of Internet Governance. Cambridge, MA: MIT Press.

Nissenbaum, H. (2005) 'Where Computer Security Meets National Security', Ethics and Information Technology, 7(2), pp. 61-73.

Nye, J.S. (2010) 'Cyber Power', Harvard Kennedy School Belfer Center for Science and International Affairs. Available at: https://belfercenter.org/publication/cyber-power (Accessed: 14 May 2024).

Rid, T. (2012) 'Cyber War Will Not Take Place', Journal of Strategic Studies, 35(1), pp. 5-32.

SANS Institute (2015) 'Critical Security Controls for Effective Cyber Defense: Version 6.0'. Available at: https://www.sans.org/critical-security-controls/ (Accessed: 15 March 2024).

Schneier, B. (2015) Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company.

Scott, J. and Spaniel, D. (2016) Malicious Cryptography: Exposing Cryptovirology. Hoboken, NJ: Wiley.

Shostack, A. (2014) Threat Modeling: Designing for Security. Indianapolis: Wiley.

Singer, P.W. (2015) 'Stuxnet and the Dawn of Algorithmic Warfare', Strategic Studies Quarterly, 9(3), pp. 17-27.

Singer, P.W. and Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press.

Skierka, I. (2017) 'The Governance of Digital Risks: A Systematic Review', Journal of Risk Research, 20(3), pp. 379-398.

Stallings, W. (2017) Network Security Essentials: Applications and Standards. 6th ed. Upper Saddle River: Pearson.

Zetter, K. (2014) Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown.