مَجَلّة الثّقَافَةِ وَالعُلُومِ لِلدِّرَاسَاتِ الإِنْسَانِيَّةِ
Culture Science Journal for Human Studies (CSJHS)

Public Cybersecurity Policies and Mobilizing International Political Cooperation: A Comparative Study between the NotPetya Ransomware Attack of 2017 and the SolarWinds Hack of 2020

Dr. Yasmine Radwan

Dr. Ayat Abdel Qader abouseeda

Introduction

Cyberthreats have become an increasingly prevalent concern in nowadays highly digitized world (McAlaney& Benson, 2019). With the advancement of technology, there are new and sophisticated ways for malicious actors to exploit vulnerabilities and gain unauthorized access to sensitive information (Khan et al., 2024). From phishing scams to ransomware attacks, the range of cyber threats is vast and constantly evolving. As a result, individuals and organizations must remain vigilant and take proactive measures to protect their digital assets. Knowing about different kinds of cyberattacks and keeping up with cybersecurity news can help us protect ourselves from online threats and reduce the chances of becoming victims of cybercrime (Martellozzo& Jane, 2017).

This paper focuses on two examples of cyberthreats, which are the NotPetya ransomware attack of 2017 and the SolarWinds Hack of 2020. Concerning the first example (the NotPetya ransomware attack of 2017), it was a widespread cyber-attack that targeted numerous organizations and institutions around the world that targeted Ukraine but spread globally, initially attributed to Russia, but the exact perpetrators remain unclear, causing significant disruption and financial losses. This attack, which was initially believed to be a variant of the Petya ransomware, turned out to be a more destructive and sophisticated form of malware that spread rapidly through networks and encrypted data on infected systems. The attackers behind the NotPetya attack employed advanced techniques to evade detection and propagate the malware, resulting in widespread chaos and confusion. The incident highlighted the growing threat of cyber-attacks and the need for organizations to strengthen their cybersecurity defenses to protect against such threats in the future (Ryan, 2021).

The second example, or the SolarWinds Hack of 2020 was a sophisticated cyberattack that targeted the software company SolarWinds, allowing hackers to

exploit its network management platform, Orion, and gain access to numerous government agencies and corporations. This unprecedented breach highlighted the vulnerability of organizations to supply chain attacks, whereby attackers compromise a trusted vendor to gain access to target networks. The impact of the SolarWinds Hack was significant, resulting in the exposure of classified government information and sensitive corporate data. It compromised several U.S. government agencies and private companies, and it is officially attributed to a Russian state-backed hacking group known as APT29 (Braw, 2022). It underscored the need for organizations to enhance their cybersecurity measures, strengthen supply chain management, and invest in advanced threat detection and response capabilities to mitigate the risk of similar attacks in the future (Issa, 2024).

Importance of the Topic

There is a significant gap in studies on activating or mobilizing international cooperation to manage or solve global challenges like cyberthreats which are complex, rapidly evolving, and often transnational in nature. This paper aims to bridge this gap by proposing a solution based on a comparative analysis of the NotPetya and SolarWinds attacks.

Research Problem

How can international cooperation be most effectively mobilized to address the evolving threat of cyberattacks, as exemplified by the NotPetya and SolarWinds incidents, and to develop a sustainable framework for global cybersecurity governance?

Hypothesis

The effectiveness of international political cooperation in cybersecurity is contingent upon the capacity and willingness of individual states to implement public policies and regulations that align with international standards

Research Questions

1- How have international norms and institutions governing cybersecurity evolved in response to these attacks?
2- What are the key challenges and opportunities for international cooperation in addressing cybersecurity threats?

3- How have public administration practices and policies changed in the wake of these incidents?
4- What are the implications of these attacks for the future of international relations and global governance?

Theoretical Framework

This paper is based on three main concepts which are; public policy, cybersecurity, and international cooperation.

1- Public Policy.

Public policy theories are essential frameworks that guide policymakers in making informed decisions and implementing effective policies to address societal issues. These theories provide a systematic approach to understanding the complexities of public policy formation, implementation, and evaluation. One of the key theories is the rational choice theory, which posits that individuals and policymakers act in their own self-interest to maximize their benefits while considering all available options. This theory helps policymakers evaluate various policy alternatives and choose the most efficient and effective solution for the public good.

Another significant public policy theory is the incrementalism theory, which suggests that policymaking is a gradual and continuous process that evolves over time through small adjustments and changes. This theory acknowledges the limitations of policymakers in making large-scale changes and emphasizes the importance of building on existing policies and making incremental improvements (Arias&, 2019).

Concerning the concept of public security policy, it offers valuable insights into the development, implementation, and evaluation of policies aimed at enhancing the safety and security of individuals and communities. One prominent theory in this field is the rational choice theory (Archer& Tritter, 2000), which posits that individuals make decisions based on a rational assessment of the costs and benefits of different courses of action. This theory is often used to explain criminal behavior and to inform policies designed to prevent and deter crime. Another important theory is the social control theory, which emphasizes the role of social institutions and relationships in regulating individuals' behavior. This theory highlights the importance of strong social bonds, such as those formed

through family, school, and community ties, in preventing delinquency and crime (Rankin& Wells, 2011).

Public security policy theories play a crucial role in shaping the approaches taken by policymakers and law enforcement agencies to address security challenges. By understanding the underlying factors that contribute to criminal behavior and insecurity, policymakers can develop more effective strategies for preventing and responding to threats to public safety. These theories also provide a framework for evaluating the impact of security policies and programs, allowing for evidence-based decision-making and the continuous improvement of security initiatives (Aslaner, 2024).

2- Cybersecurity.

Cybersecurity theories are essential in understanding and combating the ever-evolving landscape of cyber threats and attacks. One of the foundational theories in cybersecurity is the "defense-in-depth" approach, which emphasizes the use of multiple layers of security measures to protect an organization's digital assets. This theory recognizes that relying on a single security solution is not sufficient in today's complex and sophisticated cyber environment. By implementing a combination of technologies, policies, and procedures, organizations can create a more resilient defense against potential attacks (Botwright, 2024). Another important cybersecurity theory is the "Zero Trust" model, which challenges the traditional notion of trusting everything inside a network by default. This theory advocates for verifying and validating every user and device accessing the network, regardless of their location or status (Botwright, 2023). By assuming that all network traffic is potentially malicious, organizations can better protect themselves from insider threats and external attacks. The Zero Trust model also emphasizes the importance of continuously monitoring and analyzing network activity for any signs of suspicious behavior, allowing organizations to detect and respond to threats more effectively (Rais et al., 2024).

In addition to these theories, the "risk management" approach is also fundamental in cybersecurity. This theory focuses on identifying, assessing, and prioritizing potential risks to an organization's information assets and infrastructure. By understanding the potential risks and their

potential impact, organizations can make informed decisions about where to allocate resources and invest in security measures. This proactive approach to risk management helps organizations stay ahead of potential threats and vulnerabilities, minimizing the likelihood of a successful cyber-attack. Ultimately, cybersecurity theories play a crucial role in guiding organizations in their efforts to protect themselves against cyber threats and secure their digital assets in an increasingly interconnected world (Almaiah, Maleh& Alkhassawneh, 2024).

3- International Cooperation.

There are many theories that are based on international cooperation. One of the primary theories in this field is realism, which suggests that states act in their own self-interest and are primarily motivated by the pursuit of power and security. Realists argue that international cooperation is difficult to achieve due to the anarchic nature of the international system, where there is no centralized authority to enforce agreements and ensure compliance.

On the other hand, liberalism offers a more optimistic view of international cooperation, emphasizing the importance of institutions and norms in fostering collaboration among states. Liberal theorists argue that states can overcome their self-interest and work together to achieve common goals through collective action and cooperation. They believe that international organizations, such as the United Nations and the World Trade Organization, play a vital role in promoting cooperation and resolving conflicts peacefully.

Lastly, constructivism offers a different perspective on international cooperation, focusing on the role of ideas, beliefs, and identities in shaping state behavior. Constructivists argue that cooperation is not solely based on material interests, but also on shared values and norms that guide state interactions.

Approaches and Tools of Analysis

The research problem is handled by using two approaches; the political discourse analysis approach which analyses the official and non-official political speeches that tests the impact of public security policies on the activation of international political cooperation in terms of the NotPetya Ransomware Attack of

2017 and the SolarWinds Hack of 2020. The second approach is the functional approach that tests the main functions of the Ukrainian and American governments that are related to security in this regard.

These two approaches are applied through two tools of analysis which are; the desk analysis of related books, periodicals, reports and internet sources on one hand, and the content analysis in the application of the political discourse analysis.

Research Plan

1- Overview of Public Cybersecurity Policies.
2- Key Components of Effective Cybersecurity Frameworks.
3- The NotPetya Ransomware Attack of 2017: Incident Overview and Response Strategies.
4- The SolarWinds Hack of 2020: Incident Overview and Response Strategies.
5- Similarities and Differences in Attack Vectors and Techniques.
6- Mobilizing International Political Cooperation: Challenges and Opportunities.
7- Key Findings and Implications for Future Cybersecurity Policies.

1- Overview of Public Cybersecurity Policies.

Public cybersecurity policies are a set of guidelines, regulations, and standards designed to protect critical infrastructure, data, and privacy in the digital age. These policies are typically developed and implemented by governments at the national, regional, and international levels. These policies encompass a wide range of initiatives designed to protect critical infrastructure, data, and privacy in the digital age. One of the core components of these policies is critical infrastructure protection, which involves safeguarding essential services such as power grids, transportation systems, and telecommunications networks from cyberattacks. These vital systems are increasingly reliant on technology, making them vulnerable to a variety of cyber threats (Borky& Bradley, 2019).

Another critical aspect of public cybersecurity policies is data privacy and protection. Laws and regulations governing the collection, use, and storage of personal data are essential to protecting individuals' rights and preventing data breaches. With the proliferation of digital technologies and the increasing amount of personal data being collected and shared, data privacy has become a major concern.

In addition to protecting critical infrastructure and data, public cybersecurity policies also focus on preventing and combating cybercrimes. This includes laws and regulations aimed at addressing activities such as hacking, phishing, and identity theft. These cybercrimes can have serious consequences for individuals, businesses, and governments, and effective measures are needed to deter and prevent them (Watters, 2023).

International cooperation is another key component of public cybersecurity policies. Given the global nature of cyber threats, it is essential for nations to work together to address these challenges. Agreements and frameworks between countries can help establish common standards, facilitate information sharing, and coordinate responses to cyberattacks. There is no doubt that public cybersecurity policies must include strategies for risk management and resilience. This involves identifying, assessing, and mitigating cybersecurity risks, as well as building the capacity to recover from cyberattacks. By proactively addressing potential threats and developing effective resilience measures, organizations can better protect themselves against cyberattacks (Thealla et al., 2024).

The development and implementation of effective public cybersecurity policies are fraught with challenges due to the dynamic nature of the threat landscape, the technical complexity of cybersecurity issues, the complexities of international cooperation, and the potential economic impacts. One of the most significant challenges is the constantly evolving nature of cyber threats. New attack techniques, malware variants, and vulnerabilities emerge at a rapid pace, making it difficult for policies to remain relevant and effective. This requires policymakers to stay informed about the latest trends and to be adaptable in their approach (Qudrat-Ullah, 2024).

Another challenge is the technical complexity of cybersecurity issues. Understanding and addressing these issues requires specialized expertise in areas such as network security, cryptography, and digital forensics. This can be particularly challenging for smaller organizations or governments with limited resources. Coordinating cybersecurity policies and responses across different countries can also be a complex task. Varying national interests, priorities, and legal frameworks can make it difficult to reach consensus on international cooperation mechanisms. Additionally, the global nature of cyber threats means that attacks can

originate from anywhere in the world, making it challenging to attribute responsibility and coordinate responses (Bennett, 2018).

In fact, cybersecurity policies can have significant economic implications, particularly for businesses and industries that rely heavily on technology. Implementing cybersecurity measures can be costly, and the consequences of a successful cyberattack can be devastating. Balancing the need for strong cybersecurity with the economic realities of businesses and industries is a delicate task (Steinberg et al., 2023).

There are numerous public cybersecurity policies and frameworks in place around the world to address the evolving threat landscape. Some crucial examples include; the General Data Protection Regulation (GDPR) is a landmark European Union law that sets strict standards for data protection and privacy. It applies to any organization that processes the personal data of EU residents, regardless of their location. The GDPR has had a significant impact on data protection practices worldwide, and many countries have adopted similar laws. Another prominent example is the Cybersecurity Framework for Critical Infrastructure, developed by the U.S. National Institute of Standards and Technology (NIST). This voluntary framework provides a set of guidelines and best practices to help organizations identify, assess, and manage cybersecurity risks. It is widely used by both public and private sector organizations in the United States and other countries (Priyadarshini& Cotton, 2022).

At the international level, the International Telecommunication Union (ITU) Cybersecurity Framework offers guidance for countries and organizations to enhance their cybersecurity capabilities. The ITU is a specialized agency of the United Nations that focuses on information and communication technologies. Its cybersecurity framework provides a comprehensive approach to addressing cybersecurity challenges, including risk management, incident response, and international cooperation (Johnson, 2024).

2- Key Components of Effective Cybersecurity Frameworks.

A well-designed cybersecurity framework provides a structured approach to identifying, assessing, and mitigating cybersecurity risks. It serves as a roadmap for organizations to improve their security posture and protect against cyber threats. Effective cybersecurity frameworks typically include the following key components:

a- A Risk Assessment.

Risk assessment is a fundamental step in developing a comprehensive cybersecurity strategy. It involves identifying critical assets, evaluating potential threats, and determining the potential impact of those threats on the organization.

Identifying critical assets is essential for understanding the organization's vulnerabilities. This includes identifying systems, networks, data, and other resources that are essential to the organization's operations. Once critical assets have been identified, it is necessary to assess their vulnerabilities, which are weaknesses that could be exploited by attackers.

Evaluating potential threats involves identifying the various types of cyberattacks that could target the organization. This includes assessing the likelihood of different types of attacks, such as hacking, phishing, and malware infections. Understanding the potential threats facing the organization is crucial for developing effective countermeasures.

It is obvious that risk analysis involves determining the potential impact of each threat on the organization. This includes assessing the financial, operational, and reputational consequences of a successful attack. By understanding the potential impact of different threats, organizations can prioritize their security efforts and allocate resources accordingly (Talabis& Martin& 2012).

b- Governance and Management.

Effective cybersecurity requires strong leadership and a well-defined governance structure. Leadership commitment is essential for demonstrating top-level support for cybersecurity initiatives. When senior executives actively champion cybersecurity, it sends a clear message to employees that security is a priority. This can help to foster a culture of security awareness and encourage employees to report suspicious activity.

Clearly defining roles and responsibilities within the organization is another critical aspect of effective cybersecurity governance. Each employee should understand their role in protecting the organization's security, and there should be clear lines of authority and accountability. This helps to prevent confusion and ensure that security measures are implemented consistently. In fact, of establishing comprehensive cybersecurity policies and procedures is essential for providing a

framework for security activities. These policies should address a wide range of issues, including access controls, data protection, incident response, and employee training. By following these policies, organizations can ensure that their security measures are aligned with best practices and regulatory requirements (Trim& Lee, 2016).

c- Protection: Safeguarding Systems and Data.

Protection is a critical component of a comprehensive cybersecurity framework. It involves implementing measures to safeguard systems and data from unauthorized access and attacks.

- Access Controls are a fundamental aspect of protection. They are designed to limit unauthorized access to systems, networks, and data. This includes implementing strong authentication mechanisms, such as passwords, biometrics, or multi-factor authentication, to verify the identity of users before granting access. Additionally, organizations should implement authorization controls to ensure that users have only the necessary privileges to perform their job functions.
- **Network Security** involves protecting networks and systems from unauthorized access and attacks. This includes implementing firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor network traffic and detect and block malicious activity. Network segmentation can also be used to isolate critical systems and reduce the potential impact of a successful attack.
- **Data Security** is another essential aspect of protection. It involves ensuring the confidentiality, integrity, and availability of data. Confidentiality means protecting data from unauthorized disclosure, integrity means ensuring that data is accurate and complete, and availability means ensuring that data is accessible when needed. Data encryption, data loss prevention (DLP) solutions, and regular backups are key measures for protecting data (Shandilya, 2024).

d- Detection.

Detection is a critical component of a robust cybersecurity framework. It involves continuously monitoring networks and systems for suspicious activity and promptly identifying and responding to security incidents.

- Monitoring and Logging are essential for detecting potential threats. This involves using various tools and techniques to track network traffic,

system activity, and user behavior. By monitoring networks and systems, organizations can identify anomalies and potential indicators of compromise. Logging is also crucial for documenting security events and facilitating investigations.

- Incident Detection involves identifying and responding to security incidents promptly. This requires organizations to have a clear understanding of what constitutes a security incident and to have processes in place for detecting and responding to them. Incident detection systems can be used to automate the process of identifying and alerting organizations to potential threats (Kumar& Pattnaik, 2023).

e- Response.

A well-defined incident response plan is essential for organizations to effectively handle security incidents. This plan should outline the steps to be taken in the event of a cyberattack, including containment, eradication, recovery, and lessons learned. By having a clear and concise plan in place, organizations can respond to incidents in a timely and effective manner, minimizing the potential damage.

Incident handling is the process of containing and mitigating the impact of a security incident. This may involve isolating infected systems, removing malware, and restoring systems to a secure state. Effective incident handling requires a coordinated effort from various teams within the organization, including IT, security, legal, and communications.

Recovery is the final phase of the incident response process. It involves restoring systems and data to a secure and operational state. This may require rebuilding systems, restoring backups, and implementing additional security measures to prevent future attacks. A thorough recovery process is essential for ensuring business continuity and minimizing the long-term impact of a security incident (Thompson, 2018).

f- Continuous Improvement.

Continuous improvement is essential for maintaining a strong cybersecurity posture. This involves regularly assessing the effectiveness of cybersecurity measures, applying security updates and patches, and providing cybersecurity training and awareness to employees.

Monitoring and Evaluation are crucial for identifying areas for improvement. Organizations should regularly assess the effectiveness of their cybersecurity controls and identify any weaknesses or gaps. This can be done through audits, vulnerability assessments, and other evaluation methods. By monitoring and evaluating their security measures, organizations can identify areas where changes or enhancements are needed.

Updates and Patches are essential for addressing vulnerabilities in software and hardware. Security vendors regularly release updates and patches to address known vulnerabilities. Applying these updates promptly can help to protect against attacks. Organizations should have a process in place for managing updates and patches to ensure that they are applied in a timely and efficient manner.

Training and Awareness are also critical components of a strong cybersecurity program. Employees at all levels of the organization should receive training on cybersecurity best practices and be aware of the potential risks of cyberattacks. This can help to prevent employees from falling victim to phishing scams, clicking on malicious links, or inadvertently compromising the organization's security.

There is no doubt that by investing in training and awareness, organizations can empower their employees to be part of the solution and help to reduce the risk of cyberattacks (Edwards, 2024).

3- The NotPetya Ransomware Attack of 2017: Incident Overview and Response Strategies.

The NotPetya ransomware attack of 2017 was a significant cyber event that had a widespread global impact. It began in Ukraine but quickly spread to other countries, disrupting businesses, hospitals, and critical infrastructure worldwide. This attack was a self-propagating attack that encrypted files on infected systems and demanded a ransom payment. While the attack initially targeted Ukraine, its impact was widespread, affecting organizations in various sectors and countries.

The attack caused significant disruption to businesses, hospitals, and critical infrastructure worldwide. Many organizations were forced to shut down operations temporarily, leading to financial losses and operational disruptions. The attack also

highlighted the interconnectedness of the global economy and the potential for cyberattacks to have far-reaching consequences.

Organizations affected by the NotPetya ransomware attack prioritized containing the spread of the malware and isolating infected systems to prevent further damage. This involved quickly disconnecting infected devices from the network and implementing security measures to prevent the ransomware from spreading to other systems. For organizations that had implemented effective backup strategies, data recovery was a key priority. By having regular backups of their data, these organizations were able to restore their systems and data more quickly, minimizing the impact of the attack (Bochman& Freeman, 2021).

Open communication with stakeholders, including customers, employees, and regulators, was essential for managing the crisis and maintaining trust. Organizations that were transparent about the incident and provided regular updates to stakeholders were able to mitigate the negative impact of the attack and maintain their reputation. The NotPetya attack highlighted the need for robust cybersecurity measures to prevent and mitigate ransomware attacks. This includes regular backups, network segmentation, and employee training. By investing in these measures, organizations can reduce their risk of falling victim to similar attacks. In fact, the attack underscored the importance of international cooperation in addressing global cyber threats. The widespread impact of NotPetya demonstrated the need for countries to work together to share information, develop best practices, and coordinate responses to cyberattacks.

Proactive prevention involves implementing measures such as regular patch management to address known vulnerabilities, network segmentation to limit malware spread, and regular backup and recovery procedures to enable rapid data restoration in case of a breach. In the event of a ransomware attack, a swift and coordinated incident response is crucial. This includes isolating infected systems to prevent further damage, conducting a thorough forensic investigation to identify the source of the attack and gather evidence, and restoring data from backups. Additionally, implementing measures to prevent future attacks is essential.

Developing a comprehensive business continuity plan that outlines procedures for responding to and recovering from cyber security incidents is another critical aspect of preparedness. Regular testing of this plan ensures its effectiveness and helps organizations be better equipped to handle such crises (Greenberg, 2019).

4- The SolarWinds Hack of 2020: Incident Overview and Response Strategies.

The SolarWinds hack, which came to light in December 2020, was a sophisticated supply chain attack that compromised numerous government agencies and private companies worldwide. The attackers exploited a vulnerability in the SolarWinds Orion software to insert a malicious backdoor into updates, allowing them to gain unauthorized access to systems. Furthermore, the attackers were able to maintain a persistent presence in compromised systems for an extended period, making it difficult to detect and remove them.

This hack had a far-reaching impact, affecting both government agencies and private companies. Several U.S. government agencies, including the Department of Homeland Security, the Department of Treasury, and the Department of Commerce, were compromised. Additionally, numerous private companies, particularly in the technology and financial sectors, were also targeted. The attack posed a significant threat to national security as it allowed the attackers to access sensitive government information. In fact, the incident caused significant reputational damage to SolarWinds and other affected organizations (Bhardwaj, 2024).

The SolarWinds hack underscored the importance of proactive prevention and effective incident response strategies. To mitigate the risks associated with such attacks, organizations should prioritize the following measures:

- Proactive prevention involves implementing robust supply chain security measures to ensure the integrity of software updates, continuous monitoring of systems for signs of unauthorized access or suspicious activity, and regular patch management to address known vulnerabilities.
- In the event of a ransomware attack, a swift and coordinated incident response is crucial. This includes developing and implementing effective threat detection capabilities to identify and respond to attacks quickly, isolating infected systems to prevent further damage, and conducting a thorough forensic investigation to identify the source of the attack and gather evidence.

Additionally, developing a comprehensive business continuity plan that outlines procedures for responding to and recovering from cyber security incidents

is essential. Regular testing of this plan ensures its effectiveness and helps organizations be better equipped to handle such crises.

This hack was a significant cyber security incident that highlighted the vulnerabilities of supply chains and the potential for sophisticated attackers to compromise large-scale networks. By implementing proactive prevention measures, effective incident response strategies, and robust business continuity planning, organizations can better protect themselves against similar attacks (Aslaner, 2024).

5- Similarities and Differences in Attack Vectors and Techniques.

Both the NotPetya ransomware attack of 2017 and the SolarWinds hack of 2020 were significant cyber incidents with far-reaching consequences. However, they employed distinct attack vectors and techniques. In fact, these attacks shared several key similarities, such as:

- Large-scale impact: Both attacks had a profound effect, affecting numerous organizations, government agencies, and critical infrastructure. The widespread nature of these attacks highlighted the vulnerability of interconnected systems and the potential for significant disruption.
- Sophisticated adversaries: Both attacks were likely carried out by highly skilled and well-resourced adversaries, possibly state-sponsored actors. These attackers demonstrated a high level of technical expertise and a deep understanding of their targets.
- Exploitation of vulnerabilities: Both attacks exploited vulnerabilities in software or systems to gain initial access. This highlights the importance of regular software updates, vulnerability management, and patch application to prevent such breaches.

In other words, despite targeting different entities and utilizing different methods, these attacks share striking similarities in terms of their scale, sophistication, and impact. Both incidents were highly sophisticated, state-sponsored attacks that exploited vulnerabilities in widely used software to infiltrate and compromise the targeted systems. The attackers behind these incidents demonstrated advanced capabilities in reconnaissance, lateral movement, and data exfiltration, highlighting the increasingly advanced nature of cyber threats in today's digital age (Jahankhani et al., 2020).

Additionally, both attacks had far-reaching consequences that impacted organizations across various industries and geographies. The NotPetya ransomware attack, attributed to the Russian military, targeted Ukrainian infrastructure but quickly spread globally, impacting organizations in more than 65 countries. The attack resulted in billions of dollars in damages and disrupted critical services, including shipping giant Maersk and pharmaceutical company Merck. Similarly, the SolarWinds hack, believed to be orchestrated by state-sponsored Russian hackers, compromised the software supply chain of SolarWinds, leading to the infiltration of numerous government agencies and private sector organizations in the United States and beyond. Moreover, both incidents underscored the vulnerabilities inherent in interconnected digital ecosystems and the need for improved cybersecurity measures to safeguard against sophisticated cyber threats. The NotPetya ransomware attack and the SolarWinds hack exposed the reliance of modern businesses and governments on third-party software vendors and the potential risks associated with supply chain attacks. These incidents also highlighted the importance of threat intelligence sharing, incident response readiness, and proactive cybersecurity measures to detect, deter, and mitigate cyber threats effectively. In conclusion, the NotPetya ransomware attack and the SolarWinds hack serve as wake-up calls for organizations worldwide to bolster their cyber defenses and enhance collaboration efforts to combat evolving cyber threats effectively (Aslaner, 2024).

While both incidents were significant, they followed different paths, leading to distinct outcomes as follows:

- Attack vector: NotPetya was a worm that spread rapidly through networks using the EternalBlue exploit. This self-propagating nature allowed NotPetya to infect numerous systems quickly, causing widespread disruption. In contrast, the SolarWinds attack involved a supply chain attack where malicious code was inserted into the company's software updates. This technique allowed attackers to gain access to numerous organizations that relied on SolarWinds products.
- Objective: The primary objective of the NotPetya attack was to encrypt data and demand a ransom. This was a financially motivated attack aimed at extorting money from affected organizations. On the other hand, the SolarWinds attack was more targeted, aimed at espionage and intelligence gathering. This suggests that the attackers were likely state-

sponsored actors seeking to compromise government agencies and critical infrastructure.

- Impact: NotPetya caused significant disruption and financial losses due to data encryption and system downtime. Many organizations were unable to operate normally, leading to significant financial losses and operational challenges. SolarWinds, on the other hand, had a more prolonged impact as it allowed attackers to gain long-term access to compromised systems. This enabled the attackers to steal data, conduct surveillance, and potentially disrupt operations over an extended period.

To put it differently, both resulting in widespread damage and disruption to organizations and governments worldwide. One key difference between the two attacks is their primary objectives. NotPetya was designed as a destructive attack, meant to cause chaos and damage systems, while the SolarWinds hack was a more targeted, sophisticated espionage operation aimed at stealing information and gaining access to critical systems. Another major difference between the two attacks lies in their execution and impact. NotPetya spread rapidly through a software update from a legitimate Ukrainian accounting software company, infecting thousands of computers around the world and causing billions of dollars in damages. In contrast, the SolarWinds hack was a stealthy, long-term breach of a trusted software supply chain, allowing the attackers to remain undetected for months and infiltrate numerous high-profile organizations and government agencies. Additionally, the NotPetya attack was attributed to the Russian military, while the SolarWinds hack has been traced back to a Russian-based hacking group known as Cozy Bear, with suspected ties to the Russian government. The differences in attribution and motivation behind these attacks highlight the complex and evolving nature of cyber threats in today's interconnected world. As cybersecurity professionals and policymakers work to improve defenses and mitigate risks, understanding these differences and learning from past incidents will be crucial in preventing future attacks and safeguarding critical systems and infrastructure (Cavelty, 2024).

6- Mobilizing International Political Cooperation: Challenges and Opportunities.

International political cooperation is crucial in addressing global challenges such as; climate change, terrorism, and pandemics. However, mobilizing such cooperation presents numerous challenges that must be overcome in order to achieve effective and sustainable outcomes. The following part explores some of the key

challenges faced in mobilizing international political cooperation and discuss potential strategies for addressing them.

One of the primary challenges in mobilizing international political cooperation is the divergent interests and priorities of different countries. Each nation has its own agenda and concerns, making it difficult to find common ground on which to build cooperation. For example, some countries may prioritize economic growth over environmental protection, while others may prioritize national security over human rights. Understanding and acknowledging these differences is essential in order to navigate complex diplomatic negotiations and build consensus among diverse stakeholders.

Another challenge is the lack of trust and mutual respect among nations. Historical conflicts, power dynamics, and cultural differences can all contribute to mutual suspicion and animosity, making it difficult to establish a strong foundation for cooperation. Building trust and fostering positive relationships through diplomatic engagement, dialogue, and compromise is essential in overcoming this obstacle. Transparency, inclusivity, and accountability are key principles that can help promote trust and cooperation among nations.

Additionally, the rise of nationalist and isolationist sentiments in many countries poses a major challenge to international political cooperation. In an increasingly interconnected and interdependent world, isolationism can hinder progress in addressing global challenges and exacerbate existing conflicts. Overcoming nationalist tendencies and promoting a sense of shared responsibility and solidarity among nations is essential in mobilizing effective international cooperation. Leadership, vision, and persuasion are critical in rallying countries around common goals and values (Verma, Vyas& Kaushik, 2022).

Moreover, the complexity and scope of global challenges such as climate change, terrorism, and pandemics require coordinated and comprehensive responses that transcend national boundaries. Developing effective strategies for addressing these challenges requires cooperation, coordination, and collaboration among nations, as well as other stakeholders such as international organizations, non-governmental organizations, and the private sector. Building networks, partnerships, and alliances can help leverage diverse resources and expertise in tackling complex and multifaceted issues.

Mobilizing international political cooperation presents numerous challenges, but overcoming these obstacles is essential in addressing global challenges and achieving sustainable outcomes. By recognizing and understanding the divergent

interests and priorities of different countries, building trust and mutual respect, countering nationalist and isolationist sentiments, and developing comprehensive and coordinated responses, nations can work together to create a more peaceful, prosperous, and sustainable world. Effective leadership, diplomacy, and collaboration are key to mobilizing international political cooperation and fostering a culture of solidarity and mutual support among nations (Sfetcu, 2024).

Concerning the main challenges that face mobilizing international political cooperation in terms of cyberthreats, it could be summarized as follows:

a- Differing National Interests and Priorities.

One of the key challenges in mobilizing international political cooperation against cyberthreats is the divergence of national interests and priorities. Countries may prioritize economic growth and technological development over cybersecurity measures, as these factors can contribute to national prosperity and competitiveness. However, neglecting cybersecurity can lead to significant economic losses and damage to a country's reputation.

Additionally, national security concerns can hinder cooperation. Some countries may be reluctant to share sensitive information or intelligence due to fears of espionage or misuse. This reluctance can limit the effectiveness of international efforts to address cyberthreats.

Furthermore, variations in domestic laws and regulations can make it difficult to coordinate international responses to cyberattacks. Different legal frameworks may have different definitions of cybercrime, evidence standards, and enforcement mechanisms. These differences can create obstacles to cooperation and hinder the ability of countries to work together effectively (Boulet, Reiterer& Pardo, 2022).

b- Lack of Trust and Cooperation.

Another significant challenge in mobilizing international political cooperation against cyberthreats is the lack of trust and cooperation among countries. Historical tensions, past conflicts, or rivalries can create a climate of mistrust and suspicion, making it difficult for countries to work together effectively.

Geopolitical competition, particularly among great powers, can also exacerbate these tensions. In a competitive environment, countries may be more likely to view each other as adversaries rather than partners, leading to a breakdown in cooperation.

Moreover, state-sponsored cyberattacks can erode trust and undermine cooperation. These attacks can be used to steal sensitive information, disrupt critical infrastructure, and sow discord among countries. When countries suspect each other of conducting cyberattacks, it can be difficult to build the trust necessary for effective cooperation (Romaniuk& Manjikian, 2021).

c- Technological Complexity and Attribution.

The technological complexity of cyberattacks can make it difficult to identify the source of an attack, posing significant challenges to international cooperation. The sophisticated techniques used by cybercriminals and state-sponsored actors can obscure the origin of an attack, making it challenging to assign blame and pursue legal action.

Attribution disputes can also hinder cooperation. Countries may disagree over the attribution of cyberattacks, leading to diplomatic tensions and hindering international efforts to address the threat. These disputes can arise due to differing technical capabilities, political motivations, or a lack of evidence (Yannakogeorgos& Lowther, 2014).

d- Global Governance Gaps.

The fourth significant challenge in addressing cyberthreats is the lack of clear international norms and standards to govern cyberspace. This absence of a global framework can make it difficult to hold countries accountable for their actions and to coordinate responses to cyber-attacks.

Enforcing international cyber laws can also be challenging, especially in cases involving non-state actors. These actors may operate outside the jurisdiction of individual countries, making it difficult to hold them accountable. Furthermore, even when countries agree on international laws, enforcing them can be difficult due to differences in legal systems and enforcement capabilities.

Coordinating responses to cyberattacks requires cooperation among various international organizations and agencies. However, these organizations may have different mandates, priorities, and resources, which can make it difficult to achieve a unified approach (Jahankhani et al., 2024).

e- Domestic Political Constraints.

Domestic political factors can also hinder international cooperation against cyberthreats. Nationalism and isolationism may lead some

countries to prioritize domestic interests over international cooperation. This can make it difficult to build consensus on global cybersecurity issues and to implement effective international measures.

Additionally, governments may face domestic economic pressures that limit their ability to invest in cybersecurity. Economic downturns or competing priorities can make it difficult to allocate resources to cybersecurity initiatives. This can leave countries vulnerable to cyberattacks and hinder their ability to contribute to international efforts to address the threat (Buchanan, 2016).

There this no doubt that in this increasingly interconnected world, no single country can tackle these complex problems alone. Therefore, building consensus and cooperation among nations is crucial to finding effective solutions. International cooperation provides the opportunity for countries to share resources, expertise, and best practices, leading to more efficient and sustainable outcomes.

One key opportunity for mobilizing international political cooperation is through the United Nations (UN) and its various agencies, such as the World Health Organization (WHO) and the International Atomic Energy Agency (IAEA). These institutions serve as platforms for dialogue, negotiation, and cooperation among member states. For example, the Paris Agreement on climate change, which was negotiated under the UN Framework Convention on Climate Change, brought together nearly 200 countries to commit to reducing greenhouse gas emissions. This agreement demonstrates the potential of international institutions in mobilizing political cooperation on pressing global issues (Romaniuk& Manjikian, 2021).

Another opportunity for international political cooperation is through regional organizations such as the European Union (EU), African Union (AU), and Association of Southeast Asian Nations (ASEAN). These organizations provide a forum for member states to work together on common challenges and promote regional stability and development. For instance, the EU has played a key role in supporting peace and reconciliation efforts in the Balkans and promoting economic integration among its member states. Regional organizations offer a platform for countries to build trust, establish common goals, and coordinate policies, thus facilitating cooperation at the international level.

Furthermore, bilateral and multilateral partnerships among countries can also enhance international political cooperation. For example, the United States and China, despite their strategic competition, have cooperated on issues such as climate change, North Korea, and public health. These partnerships demonstrate that even

countries with divergent interests can find common ground and work together for mutual benefit. Multilateral platforms, such as the G7, G20, and BRICS, also offer opportunities for countries to collaborate on global economic, security, and development challenges.

In conclusion, mobilizing international political cooperation opportunities is essential for addressing the complex and interconnected challenges facing the world today. Through the United Nations, regional organizations, bilateral partnerships, and multilateral platforms, countries can work together to find common solutions, build trust, and promote global stability and prosperity. By seizing these opportunities for cooperation, nations can create a more peaceful, sustainable, and inclusive world for future generations.

Concerning cyberthreats as a global challenge, there are significant opportunities for international cooperation in addressing it, such as; shared threats, economic interdependence, technological advancements, international institutions, global civil society, and public-private partnerships (Johnson, 2024).

a- Shared Threats.

Cyberattacks can have far-reaching consequences, affecting critical infrastructure, economies, and national security. These threats pose a significant challenge to global stability and prosperity. Recognizing the shared nature of these threats can motivate countries to work together to develop and implement effective cybersecurity measures. Based on this opportunity, countries can understand that their own security is closely linked to the security of others. This shared understanding can foster cooperation and encourage countries to work together to address common threats (Skopik, 2018).

b- Economic Interdependence.

The interconnectedness of global supply chains makes countries vulnerable to cyberattacks. Disruptions to these supply chains can have significant economic consequences, affecting everything from manufacturing to retail. Cyberattacks that target critical infrastructure or supply chain components can disrupt the flow of goods and services, leading to economic losses and disruptions.

To mitigate these risks, countries can work together to protect critical infrastructure and supply chains. This includes sharing information about cyber threats, developing joint cybersecurity initiatives, and implementing

best practices for protecting critical infrastructure. The fact of working together leads countries to strengthen their collective resilience to cyberattacks and minimize the economic impact of such incidents (Shackelford, 2014).

c- Technological Advancements.

Technological advancements can play a crucial role in addressing cyberthreats and facilitating international cooperation. Advanced technologies can facilitate the sharing of threat intelligence and best practices among countries. This information sharing can help countries stay informed about emerging threats, identify vulnerabilities, and develop effective countermeasures.

Additionally, countries can collaborate on research and development of cybersecurity technologies. By working together, countries can pool their resources and expertise to develop innovative solutions to address cyber threats. This collaboration can also help to level the playing field, as it can enable smaller countries to access advanced technologies and capabilities (Benson& McAlaney, 2019).

d- International Institutions.

International institutions can play a crucial role in facilitating international cooperation against cyberthreats. Existing frameworks, such as the United Nations, the G7, and the G20, can provide platforms for countries to discuss cybersecurity issues, develop common standards, and coordinate responses to cyberattacks.

However, addressing the unique challenges posed by cyberthreats may require the creation of new international institutions or mechanisms. These specialized bodies can focus on specific cybersecurity issues, develop tailored norms and standards, and promote international cooperation. For example, a dedicated international cybersecurity agency could coordinate information sharing, facilitate incident response, and promote capacity building among countries (Romaniuk& Manjikian, 2021).

e- Global Civil Society.

Global civil society organizations can play a vital role in addressing cyberthreats and promoting international cooperation. These organizations can raise awareness of cyber threats and advocate for stronger international cooperation. By highlighting the risks posed by cyberattacks and the need

for coordinated action, civil society organizations can mobilize public opinion and pressure governments to take action.

Additionally, NGOs can provide training and capacity building to developing countries. Many developing countries lack the resources and expertise to effectively address cyber threats. By providing training and technical assistance, NGOs can help these countries improve their cybersecurity capabilities and reduce their vulnerability to attacks. This can help to level the playing field and ensure that all countries have the ability to contribute to international efforts to combat cybercrime (Kshetri, 2010).

f- Public-Private Partnerships.

Public-private partnerships can play a crucial role in addressing cyberthreats. Governments and private sector companies can work together to develop and implement cybersecurity solutions. This collaboration can leverage the expertise of both the public and private sectors to identify vulnerabilities, develop effective countermeasures, and share best practices.

Public-private partnerships can also help to share resources and expertise. Governments can provide funding and regulatory support, while private sector companies can contribute their technical expertise and innovative solutions. By working together, governments and private sector companies can more effectively address the complex challenges posed by cyber threats (Awan& Blakemore, 2016).

In addition to these opportunities, there are many scholars who test public security policies as an opportunity that could help in mobilizing international political cooperation and mitigate cyber threats, and they found that public security policies, particularly those related to law enforcement, intelligence, and critical infrastructure protection, can play a significant role in mobilizing international political cooperation to mitigate cyber threats. By establishing effective domestic frameworks and collaborating with international partners, countries can enhance their cybersecurity capabilities and contribute to a more secure global cyberspace by applying some important tools, such as; **first- establishing legal frameworks**- One of the key components of a robust cybersecurity strategy is the establishment of comprehensive legal frameworks. Countries can develop domestic laws and regulations to address cybercrime, protect critical infrastructure, and regulate the use of technology. These laws can provide a legal basis for law enforcement agencies to

investigate and prosecute cybercrimes, as well as for businesses and individuals to comply with cybersecurity requirements. Furthermore, countries can work together to develop international standards and best practices for cybersecurity. These standards can provide a common framework for countries to follow, ensuring a more consistent and effective approach to addressing cyber threats. By harmonizing their legal frameworks and adopting international standards, countries can improve their ability to cooperate and share information effectively. **Second- Enhancing Law Enforcement Capabilities** that could help in effectively combatting cybercrime through countries which must invest in the training and capacity building of their law enforcement agencies. In fact, providing law enforcement personnel with the necessary skills and knowledge help countries to improve their ability to investigate and prosecute cybercrimes. This includes training on digital forensics, network security, and international law. In addition to domestic training, law enforcement agencies can benefit from international cooperation. By collaborating with their counterparts in other countries, law enforcement agencies can share information, coordinate investigations, and extradite cybercriminals. This can help to dismantle transnational cybercrime networks and bring perpetrators to justice. **Third- Protecting Critical Infrastructure**, such as; power grids, transportation networks, and financial systems, is essential to the functioning of modern societies. Protecting this infrastructure from cyberattacks is a top priority for governments around the world. Countries can conduct risk assessments of their critical infrastructure to identify vulnerabilities and prioritize protection measures. By understanding the potential risks, countries can implement appropriate security measures to mitigate the likelihood and impact of cyberattacks. Furthermore, countries can work together to develop and adopt international standards for critical infrastructure protection. These standards can provide a common framework for countries to follow, ensuring a more consistent and effective approach to protecting critical infrastructure. By harmonizing their protection measures, countries can improve their resilience to cyber threats and reduce the risk of widespread disruptions. **Finally- Intelligence Sharing and Cooperation** are essential for effectively addressing cyber threats. Intelligence agencies can share information about cyber threats, vulnerabilities, and potential attacks. This sharing can help countries stay informed about emerging threats, identify vulnerabilities, and develop effective countermeasures. In addition to sharing information, intelligence agencies can collaborate on joint operations to disrupt cybercrime networks and dismantle state-sponsored hacking groups. These operations can involve sharing resources, expertise, and intelligence to identify and

target cybercriminals. By working together, intelligence agencies can more effectively combat cyber threats and protect critical infrastructure (Sharma, 2024).

7- Key Findings and Implications for Future Cybersecurity Policies.

The NotPetya ransomware attack of 2017 and the SolarWinds Hack of 2020 were two significant cyber incidents that highlighted the growing threat of cyberattacks and the need for enhanced cybersecurity measures. These attacks demonstrated the potential for cyber threats to cause widespread disruption, financial losses, and damage to national security. The study found that international political cooperation is essential for addressing the evolving threat of cyberattacks. By working together, countries can share information, develop best practices, and coordinate responses to cyber threats. However, effective international cooperation requires strong public cybersecurity policies and capabilities. The analysis of the NotPetya and SolarWinds incidents revealed that the effectiveness of international cooperation is contingent upon the capacity and willingness of individual states to implement public policies and regulations that align with international standards. Countries must invest in cybersecurity infrastructure, develop legal frameworks, and enhance the capabilities of their law enforcement agencies to contribute to global cybersecurity efforts. In conclusion, the study emphasizes the importance of public cybersecurity policies and international cooperation in mitigating cyber threats. By strengthening domestic cybersecurity measures and working together on a global scale, countries can better protect themselves from the risks posed by cyberattacks and ensure a more secure and resilient digital future.

The implications for future cybersecurity policies could be noticed at the national and the international level. Concerning the national level, organizations should conduct regular risk assessments to identify vulnerabilities and prioritize protection measures. By understanding the potential risks facing their organization, they can develop tailored strategies to mitigate those risks and protect their assets. This includes implementing security controls, educating employees, and developing incident response plans. By proactively addressing risks, organizations can reduce their exposure to cyber threats and improve their resilience. At the international level, governments should mainly work together to address the vulnerabilities of global supply chains and ensure the security of software and hardware. This includes developing standards for supply chain security, conducting audits of suppliers, and promoting the use of secure software development practices. By addressing supply chain vulnerabilities, countries can reduce the risk of cyberattacks that target critical

infrastructure and disrupt essential services. Additionally, developed countries should support capacity building efforts in developing countries to help them improve their cybersecurity capabilities. This includes providing training, technical assistance, and financial support. By building the capacity of developing countries, governments can help to reduce the global vulnerability to cyber threats and ensure a more equitable and secure digital landscape.

Recommendations for Future Research:

Based on the findings of this study, the following recommendations are offered for future research:

- Comparative analysis of additional cyber incidents: Conduct a comparative analysis of more recent cyber incidents to identify emerging trends, challenges, and opportunities for international cooperation.
- Case studies of successful international cooperation: Explore specific case studies of successful international cooperation in addressing cyber threats to identify best practices and lessons learned.
- Evaluation of the effectiveness of existing international institutions: Assess the effectiveness of existing international organizations and mechanisms in addressing cyber threats and identify areas for improvement.
- Analysis of the role of non-state actors: Examine the role of non-state actors, such as cybercrime groups and hacktivists, in the cyber threat landscape and assess the effectiveness of international cooperation in addressing their activities.
- Longitudinal studies of cybersecurity trends: Conduct longitudinal studies to track changes in the cyber threat landscape, the effectiveness of cybersecurity policies, and the evolution of international cooperation.
- Interdisciplinary research: Encourage interdisciplinary research to draw on insights from various fields, such as law, economics, sociology, and psychology, to better understand the complexities of cyber threats and develop effective countermeasures.
- Public opinion surveys: Conduct public opinion surveys to gauge public awareness of cyber threats, trust in government institutions, and support for international cooperation.

- Ethical considerations: Examine the ethical implications of cybersecurity policies and practices, including issues such as surveillance, privacy, and human rights.

By conducting further research in these areas, scholars can contribute to a deeper understanding of the challenges and opportunities for international cooperation in cybersecurity and inform the development of more effective policies and strategies.

List of References

1- Almaiah, M., Maleh, Y.& Alkhassawneh, A. (2024). *Risk assessment and countermeasures for cybersecurity*. IGI Global: USA.
2- Arias, R. D. G. (2019). Public Policies Between Theory and Practice. *Ánfora*, *26*(46), 191-216.
3- Aslaner, M. (2024). *Cybersecurity Strategies and Best Practices: A Comprehensive Guide to Mastering Enterprise Cyber Defense Tactics and Techniques*. Packt Publishing L.t.d.: UK.
4- Awan, I.& Blakemore, B. (2016). *Policing cyber hate, cyber threats and cyber terrorism*. Routledge: USA.
5- Bhardwaj, A. (2024). *Insecure digital frontiers: Navigating the global cybersecurity landscape*. CRC Press: USA
6- Bennett, B. (2018). *Understanding, assessing, and responding to terrorism: Protecting critical infrastructure and personnel*. Wiley: USA.
7- Benson, V.& McAlaney, J. (Eds.). (2019). *Emerging cyber threats and cognitive vulnerabilities*. Academic Press.
8- Bochman, A.& Freeman, S. (2021). *Countering cyber sabotage introducing consequence-driven, cyber-informed engineering (CCE)*. CRC Press: USA.
9- Borky, J.& Bradley, T. (2019). *Effective model-based systems engineering*. Springer International Publishing: Switzerland.
10- Botwright, R. (2024). *Defense in depth: Network security and cyber resilience*. Library of Congress.
11- Botwright, R. (2023). *Zero trust security: Building cyber resilience& robust security postures*. Library of Congress.
12- Boulet, G., Reiterer, M.& Pardo, R. (2022). *Cybersecurity policy in the EU and South Korea from consultation to action: Theoretical and comparative perspectives*. Springer International Publishing: Switzerland.
13- Braw, E. (2022). *The Defender's Dilemma: Identifying and Deterring Gray-zone Aggression*. Rowman & Littlefield.
14- Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press: England.
15- Cavelty, M. (2024). *The politics of cyber-security*. Routledge: USA.

16- Edwards, J. (2024). *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley& Sons Ltd.: USA.
17- Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Knopf Doubleday Publishing Group: USA.
18- Issa, T. (2024). *Management Information Systems: Harnessing Technologies for Business& Society*. Sage.
19- Jahankhani, H. et al. (eds.). (2024). *Space governance: Challenges, threats and countermeasures*. Springer International Publishing: Switzerland.
20- Jahankhani, H. et al. (eds.). (2020). *Cyber defence in the age of AI, smart societies and augmented humanity*. Springer International Publishing: Switzerland.
21- Johnson, D. (2024). *Leadership fundamentals for cybersecurity in public policy and administration: Lessons for the global south*. Routledge: New York.
22- Khan, I. U. et al. (Eds.). (2024). *Cyber security for next-generation computing technologies*. CRC Press: USA.
23- Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives*. Springer Science & Business Media.
24- Kumar, R.& Pattnaik, P. (2023). *Risk detection and cyber security for the success of contemporary computing.* IGI Global: USA.
25- Martellozzo, E.& Jane, E. A. (Eds.). (2017). *Cybercrime and its victims*. Taylor & Francis.
26- Peggs, K.& Lampard, R. (2013). Rational Choice Theory: Resisting Colonization, (in) Archer, M.& Tritter, J. (eds.), *Rational choice theory: Resisting colonization*, pp. 93- 110. Routledge: New York.
27- Priyadarshini, I.& Cotton, C. (2022). *Cybersecurity: Ethics, legal, risks, and policies*. Apple Academic Press: USA.
28- Qudrat-Ullah, H. (2024). *Sustainable energy: A myth or reality*. Springer: Switzerland.
29- Rankin, J.& Wells, E. (2016). *Social control and self-control theories of crime and deviance*. Routledge: New York.
30- Romaniuk, S.& Manjikian, M. (2021). *Routledge companion to global cyber-security strategy*. Routledge: New York.
31- Ryan, M. (2021). *Ransomware Revolution: the rise of a prodigious cyber threat* (Vol. 85). Berlin/Heidelberg, Germany: Springer.
32- Sfetcu, N. (2024). *Advanced persistent threats in cybersecurity – Cyber warfare*. MultiMedia Publishing: Canada.
33- Shackelford, S. (2014). *Managing cyber attacks in international law, business, and relations: In search of cyber peace*. Cambridge University Press: USA.
34- Shandilya, S. et al. (2024). *Digital resilience: Navigating disruption and safeguarding data privacy*. Springer: Switzerland.
35- Sharma, A. (2024). *Cyber- An era of crime& laws*. Blue Rose Publishers: India.
36- Skopik, F. (2018). *Collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks at the national level*. CRC Press: USA.
37- Steinberg et al. (2023). *Cybersecurity all-in-one for dummies*. John Wiley& Sons, Inc.: New Jersey.

38- Talabis, M.& Martin, J. (2012). *Information security risk assessment toolkit: Practical assessments through data collection and data analysis*. Elsevier: USA.
39- Thealla, P. et al. (eds.). (2024). *Corporate cybersecurity in the aviation, tourism, and hospitality sector*. IGI Global: USA.
40- Thompson, E. (2018). *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*. Apress: USA.
41- Trim, P.& Lee, Y. (2016). *Cyber security management: A governance, risk and compliance framework*. Routledge: USA.
42- Verma, S., Vyas, V.& Kaushik, K. (2022). *Cybersecurity issues, challenges, and solutions in the business world*. IGI Global: USA.
43- Watters, P. (2023). *Cybercrime and cybersecurity*. CRC Press: USA.
44- Yannakogeorgos, P.& Lowther, A. (2014). *Conflict and cooperation in cyberspace: The challenge to national security*. Taylor& Francis: UK.