information

Review

Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era

Aisha Adeyeri and Hossein Abroshan *

School of Computing and Information Sciences, Anglia Ruskin University, Cambridge CB1 1PT, UK
* Correspondence: hossein.abroshan@aru.ac.uk

Abstract: As the digital environment progresses, the complexities of cyber threats also advance, encompassing both hostile cyberattacks and sophisticated cyber espionage. In the face of these difficulties, cooperative endeavours between state and non-state actors have attracted considerable interest as crucial elements in improving global cyber resilience. This study examines cybersecurity governance's evolving dynamics, specifically exploring non-state actors' roles and their effects on global security. This highlights the increasing dangers presented by supply chain attacks, advanced persistent threats, ransomware, and vulnerabilities on the Internet of Things. Furthermore, it explores how non-state actors, such as terrorist organisations and armed groups, increasingly utilise cyberspace for strategic objectives. This issue can pose a challenge to conventional state-focused approaches to security management. Moreover, the research examines the crucial influence of informal governance processes on forming international cybersecurity regulations. The study emphasises the need for increased cooperation between governmental and non-governmental entities to create robust and flexible cybersecurity measures. This statement urges policymakers, security experts, and researchers to thoroughly examine the complex relationship between geopolitics, informal governance systems, and growing cyber threats to strengthen global digital resilience.

Keywords: cybersecurity; digital warfare; geopolitical ramifications; information governance; information management; security threats; governmental regulations

Citation: Adeyeri, A.; Abroshan, H. Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information* **2024**, *15*, 682. https://doi.org/10.3390/info15110682

Academic Editor: Krzysztof Szczypiorski

Received: 17 September 2024
Revised: 17 October 2024
Accepted: 23 October 2024
Published: 1 November 2024

1. Introduction

The landscape of cybersecurity governance models involves interactions among stakeholders illustrating a range of cyber threats and vulnerabilities. The model relies on communication between government officials and those outside government organisations. Their efforts are seen as crucial for combating cyber dangers [1]. Multi-stakeholder cyber diplomacy enables collaboration among stakeholder sectors to enhance the effectiveness of initiatives. The absence of established systems underscores the need for innovative approaches to tackle emerging cyber threats, such as changes and the rise of non-governmental actors impacting diplomatic relations. Informal collaborations complement hierarchical structures, underlining the importance of flexible governance methods [2]. These insights reveal the ever-changing nature of cybersecurity governance, where both state and non-state actors play roles in addressing cyber threats and vulnerabilities. The interactions among these parties influence the development and implementation of cybersecurity policies and plans, underscoring the importance of collaborative approaches in tackling cyber challenges. For example, China's cybersecurity governance framework has been influenced by its political, social, and economic contexts, resulting in strategies and laws to safeguard its digital domain [3]. By adopting a stakeholder approach to cybersecurity, China promotes the involvement of stakeholders, including government agencies, businesses, and civil society organisations. This cooperative strategy enhances our understanding of cybersecurity governance complexities and the challenges of navigating geopolitical

landscapes. It is worth noting that the European Union and the United States have distinct legal, regulatory, and organisational laws governing cybersecurity, which are influenced by their historical, cultural, and geopolitical differences [4]. The EU prioritises coordination among member nations, whereas the US framework emphasises partnerships between the public and private sectors and industry-led initiatives. Examining the geopolitical dimensions of multi-stakeholder cyber diplomacy offers insights into the intricate relationship between geopolitical cybersecurity policies and international affairs. Cybersecurity governance touches on geopolitical factors beyond operational concerns and is tied to broader geopolitical trends. Hence, grasping the geopolitical dimensions of cybersecurity governance is essential for shaping policies and strategies that can adjust to geopolitical landscapes [5].

Furthermore, Public–Private Partnerships (PPPs) are now acknowledged as a critical approach to enhancing infrastructure resilience against cyber threats [6]. By facilitating information sharing resource allocation and response coordination, PPPs leverage expertise and resources from both the public and private domains. PPPs encourage an approach to cybersecurity by promoting collaboration and a shared sense of accountability among stakeholders. This framework encompasses technical measures, policy formulation, governance practices, and risk management tactics to tackle cyber challenges. In the dynamic cyber threat landscape, PPPs offer an adaptable framework to address these intricacies. Ultimately, such partnerships can strengthen the resilience of critical infrastructure in the world. This study examines the dynamics in cybersecurity governance, with a focus on the role of actors in fostering cooperation and enhancing cyber resilience. The aim is to explore the responsibilities, contributions, challenges, and effects of state–non-state actor partnerships through a literature review method. This review delves into how countries and international organisations comprehensively address cyber threats, focusing on various geopolitical ramifications, such as differences in technology, governance, cooperation, etc. By studying themes and publications, this research seeks to shed light on the complex dynamics shaping the digital warfare landscape and provide insights into governance practices. Moreover, because digital warfare involves various issues of strategy, policy, corporations, etc., which impact cyberattacks and defences [7], this study focuses on digital warfare.

The next sections of this paper present and analyse the various aspects and studies about cyber war and warfare provided by the research community. Section 2 explains the methodology we used in this study. Section 3 is a holistic literature review of the topic. Section 4 explains three short case studies, and Section 5 discusses the findings and proposes future studies and some recommendations to organisations and governments (e.g., policymakers).

2. Methodology and Data Collection

This study employed a literature review methodology to investigate how state and non-state actors work together in cybersecurity governance. The review involved analysing various academic works and research findings connected to a specific area of interest. The review served as a framework for acquiring, assessing, and integrating information regarding collaborative efforts within cybersecurity governance. Creating a search strategy, formulating research questions, establishing criteria for study selection, reviewing and choosing relevant research and data, and evaluating the quality of studies were all crucial steps in conducting the literature review. Collecting a mix of evidence was crucial to understanding the roles, impacts, obstacles, and results of state and non-state actor partnerships in enhancing cybersecurity worldwide. Through this process, we aimed to highlight obstacles and detect patterns and zones for further investigation. Ultimately, this could inform the development of policies, research projects, and practical steps to enhance cooperation in cybersecurity on a global level.

In the thematic organisation phase, the collected data were systematically categorised based on themes to reveal patterns, trends, and reoccurring issues found in the litera-

ture [8]. A qualitative data analysis was performed to clarify the collaborative dynamics between state and non-state actors in cybersecurity governance. This synthesis entailed a comprehensive analysis and interpretation of the thematic patterns and trends revealed in the literature.

The data collection approach for this scientific literature review was undertaken diligently to ensure that all relevant material was found and included. The approach was outlined in the following steps.

Comprehensive Search: To ensure a comprehensive investigation, a thorough search of academic databases and scholarly repositories was conducted to find relevant peer-reviewed publications, conference papers, and research reports. The search used prominent databases such as PubMed, Scopus, IEEE Xplore, Google Scholar, and Web of Science.

Keyword Searches: Terms related to cybersecurity, cooperation, non-state actors, state actors, and governance were combined in the keyword searches. Based on each database's search capabilities, these keywords were tailored to optimise the retrieval of relevant literature.

Inclusion/Exclusion Criteria: As Table 1 shows, specific inclusion and exclusion criteria were developed to help select relevant material. The relevance of the research topics, the publication date, the language, and the study design were the criteria for selection, guaranteeing that only articles of superior quality and relevance were incorporated into the review, aligning with the predetermined criteria and the overarching focus on cybersecurity governance.

Table 1. Inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Publications accessible in the English language	Publications that were not accessible in the English language.
Research conducted on cybersecurity includes empirical investigations, theoretical frameworks, case studies, analysis, and reviews.	None
To maintain relevance, publications dated between 2016 and 2024.	None
Articles that discuss the main ideas given in the research question.	None

Using EndNote (version 20) for reference management was pivotal in maintaining a structured and efficient approach to handling citations and organising the vast array of articles collected during the search process. This methodical literature management served as a foundational element in assembling a robust and well-informed scholarly review, enabling the synthesis and interpretation of thematic patterns and trends within the literature to underpin the research's comprehensive analysis of cybersecurity governance.

Categorisations: Using the keyword search, over 300 relevant publications were investigated. Considering relevance to the study topic, 64 publications were selected for this work. After carefully considering the 64 papers and attempts to categorise them, 57 papers were chosen due to their alignment with the essential areas deemed crucial for the study. This indicates that seven papers were excluded from the screening process. The criteria for selection included how well the paper fits with the main ideas, theoretical frameworks, empirical evidence, analysis, advocacy, and practical solutions needed for a full review of the cybersecurity landscape. Figure 1 illustrates the publication years of the papers. As it shows, most of the selected articles were published recently.

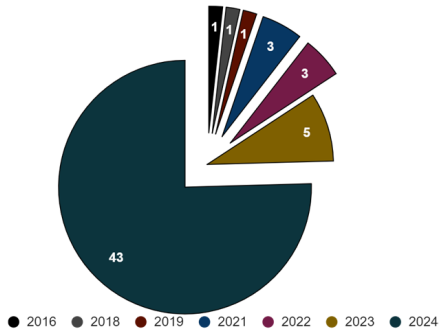

Figure 1. Year of publication.

For each search, thorough searches were made on Google Scholar and other scholarly databases, such as PubMed, IEEE Xplore, and the ACM Digital Library. The search keywords were customised for each inquiry to assure relevancy and comprehensiveness. Papers were selected based on their pertinence to the research inquiries and adherence to the predetermined criteria. The search criteria, such as analysis of endeavours, case studies demonstrating achievements, obstacle identification, examples of used search keywords, etc., are captured in Table 2.

Table 2. Overview of search focuses and alignment of criteria.

Focus Areas	Search Criteria and Search Keywords
Evolving cybersecurity threats in the digital warfare era	Identification and analysis of significant cybersecurity risks; Examination of the dynamic nature of cyber threats keywords: “cyber threats”, “digital warfare”
Traditional state-centric approaches to cybersecurity	An examination of conventional state-led cybersecurity measures and an evaluation of their inherent shortcomings. keywords: “cybersecurity measures”, “governmental approach”, “state-centric”
The rise of non-state actors in cybersecurity	Overview of non-state actors; Analysis of distinctive capacities keywords: “cybersecurity”, “non-state actors”, “warfare”, “capacities”
Contributions of non-state actors to cybersecurity	Analysis of endeavours; Case studies demonstrating achievements keywords: “contribution”, cybersecurity”, “non-state actors”, “warfare”
Challenges faced by non-state actors	Obstacle identification; Analysis of limitations in resources, legal impediments, and coordination difficulties keywords: “cybersecurity challenges”, “non-state actors”, “warfare”
Impact of non-state actors in the cybersecurity landscape	Evaluation of the impact on societal norms and policies; Assessment of the efficacy keywords: “cybersecurity”, “impacts”, “non-state actors”
Enhancing collaboration between state and non-state actors	Potential avenues for collaboration; Suggestions for establishing relationships keywords: “cybersecurity”, “collaborations”, “non-state actors”, “state actors”
Technological solutions and innovations	Technological solutions overview; Emerging technologies analysis keywords: “cybersecurity”, “technical solutions”, “innovations”, “warfare”

The considered focused areas help us understand solutions to tackle cyber threats in digital warfare. Figure 2 shows how the focused areas are linked together and support our analyses.

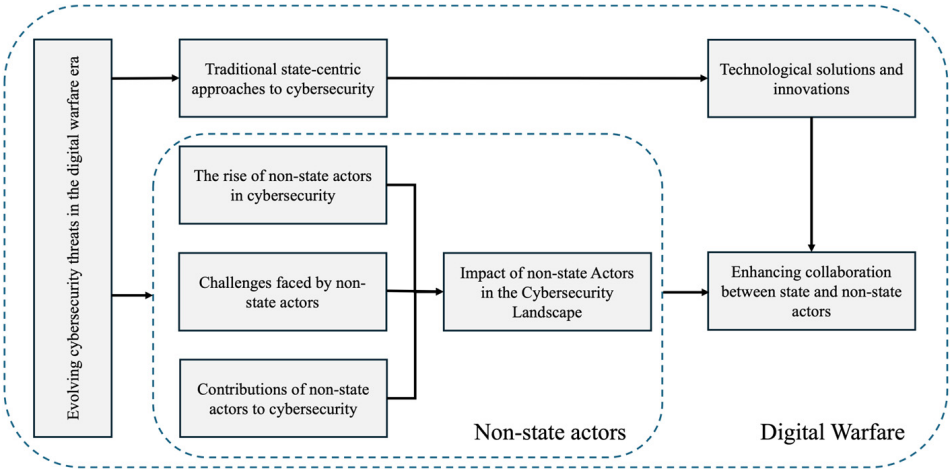

Figure 2. Relationships between the focused areas.

By organising the themes in coherence with the main research questions, this research paper establishes a framework for comprehensive exploration, analysis, and integration of information pertinent to the evolving dynamics of cybersecurity governance. This thematic organisation enables a structured and focused approach to address the intricate relationship between geopolitics, informal governance systems, and growing cyber threats, ultimately enhancing global digital resilience.

The identified themes include:

Cooperative Endeavours in Cybersecurity Governance: This theme delves into the collaborative efforts between state actors and non-state actors, emphasising the role of international non-governmental organisations, business sector entities, and civil society organisations in enhancing global cyber resilience. It directly relates to the research question exploring the effectiveness of cooperative endeavours in improving global cyber resilience.

Emerging Cyber Threat Landscape: This theme encapsulates the evolving nature of cyber threats, including supply chain attacks, advanced persistent threats, ransomware, and vulnerabilities on the Internet of Things. It aligns with the research question seeking to understand the increasing dangers posed by contemporary cyber threats and their impact on global security governance.

Non-state Actors and Strategic Utilisation of Cyberspace: This theme explores how non-state actors, including terrorist organisations and armed groups, leverage cyberspace for strategic objectives. It sheds light on the growing significance of non-state actors in the cybersecurity domain. It directly connects to the research question examining the effects of non-state actors on global security and their implications for conventional state-focused security management approaches.

Informal Governance Processes and International Regulations: This theme emphasises the influential role of informal governance processes in shaping international cybersecurity regulations. It relates to the research question investigating the crucial influence of informal governance on forming international cybersecurity regulations and underscores the need for increased cooperation between governmental and non-governmental entities to develop robust cybersecurity measures.

3. Literature Review

Cybersecurity concerns are essential in shaping global politics and bringing risks to aspects such as national security stability and public well-being. Technology's progress and reliance on connected ICT systems have resulted in a rise in cyberattacks carried out by

various state and non-state actors. Understanding the impact of these dangers is essential in an era where the line between the physical and digital realms is becoming increasingly blurred. This research explores how countries and entities address cyber threats, focusing on their efforts. By examining common themes and the existing literature, this study aims to help untangle the complexities of the cyber landscape while providing insights into effective governance practices.

3.1. Evolving Cybersecurity Threats in the Digital Warfare Era

In the digital warfare era, the increasing dependence on information and communication technology (ICT) infrastructure has led to remarkable interconnectedness, facilitating everyday life. However, this dependence also introduces significant vulnerabilities that malicious actors exploit, posing grave security risks [9]. Cybersecurity threats have become more sophisticated and targeted. The impact of these threats on the geopolitical landscape is significant, as state and non-state actors increasingly use cyber capabilities to pursue their strategic objectives and undermine the security of rival nations [10].

Among the variety of risks facing ICT infrastructure, advanced persistent threats (APTs), ransomware, and supply chain attacks stand out as particularly menacing adversaries. Understanding the nature of these dangers is essential for creating efficient defence tactics to protect sensitive data and vital systems [7]. For example, the APT group known as "Fancy Bear" has been linked to numerous high-profile attacks targeting government agencies and political organisations [11]. Advanced Persistent Threats (APTs) are complex cyberattacks carried out by skilled attackers with significant resources and skills [12]. Advance Persistence Threats (APTs) are known for being secretive and long-lasting, as malicious individuals use sophisticated methods to breach specific networks, steal confidential information, and sustain unnoticed entry for extended periods [13]. The multilayered campaigns usually start with thorough reconnaissance efforts to identify vulnerabilities and potential entry sites. Attackers then carry out the initial breach using techniques such as spear phishing or other social engineering approaches. After infiltrating the network, attackers move horizontally and increase their access rights, enhancing their authority and enabling activities like espionage, the theft of intellectual property, or disruption [14]. APTs differ from traditional cyberattacks by employing a sophisticated approach that involves patience, precision, and strategic navigation of networks to achieve objectives while avoiding detection. APTs can develop a strong presence in targeted locations due to their secretive and persistent characteristics, which allow them to conduct long-term surveillance, steal data, and carry out hidden operations [15]. APTs can bypass conventional security measures by using sophisticated methods and taking advantage of weaknesses, which poses challenges for companies in terms of identification and mitigation [13]. APTs frequently exhibit a strong ability to adapt, constantly changing their methods and approaches to bypass protective measures and take advantage of new weaknesses [12,13]. To address this dynamic nature, organisations must deploy proactive cybersecurity measures such as continuous monitoring, threat intelligence exchange, and effective defence-in-depth tactics [16]. Actors can reduce the risk of APTs by strengthening their resilience and improving their detection skills, therefore protecting their digital assets and infrastructure against complex cyber assaults.

Ransomware has become a widespread and disruptive cyber threat that targets enterprises in several sectors via encryption-based extortion methods [13]. The WannaCry ransomware attack in 2017, which affected over 200,000 computers across 150 countries, is a prime example of the devastating impact of ransomware [17]. Cybercriminals use phishing emails or exploit kits to acquire unauthorised access to a victim's network in a ransomware attack. Upon gaining access, they utilise advanced encryption algorithms to make important data or systems unreachable, essentially keeping them captive. Afterwards, the attackers request money, typically in cryptocurrency, in return for decryption keys or the commitment to unlocking the encrypted data. Ransomware versions have evolved to use complex evasion strategies such as polymorphic malware and file-less attacks to bypass

traditional security measures, making identification and prevention more challenging [18]. Polymorphic malware changes its code with each infection, making it difficult for antivirus tools to identify, while file-less attacks use genuine system processes to run harmful payloads without conventional traces [19]. Organisations should use multilayered protection techniques and strong backup and recovery processes to reduce the danger of ransomware attacks, as these tactics make ransomware threats more sophisticated and powerful.

Supply chain attacks have increased recently, with malicious individuals targeting suppliers, vendors, and partners to undermine the quality of products, services, or infrastructure [12]. The SolarWinds breach in 2020, which affected numerous government agencies and private companies, is a prime example of the devastating impact of supply chain attacks [20]. These covert attacks take advantage of weaknesses in the supply chain to breach secure networks, spread harmful software, or tamper with trusted software updates, creating substantial risks for enterprises and their stakeholders [18]. Organisations must implement a proactive strategy for managing supply chain risks, which involves thoroughly evaluating vendors, enhancing supply chain transparency, and developing plans for responding to incidents. Organisations may reduce the effect of supply chain attacks and strengthen the resilience of their operations by improving their defences and working closely with partners and industry peers.

APT, ransomware, and supply chain attacks are significant cybersecurity risks that need proactive steps to reduce their impact efficiently. Actors can improve their ability to withstand and protect against emerging cyber threats by comprehending threat actors' strategies, methods, and protocols and establishing strong security measures [21]. Collaboration, information sharing, and continual monitoring are crucial to combating the ever-changing cyber threats and protecting ICT infrastructure in a more linked world.

3.2. Traditional State-Centric Approaches to Cybersecurity

Historically, cybersecurity strategies and policies have been greatly shaped by approaches emphasising the role of governments in safeguarding national interests and critical infrastructure from cyberattacks. These methods prioritise leveraging power and assets to establish an integrated framework for addressing cyber threats and minimising risks to security. Despite their effectiveness, such approaches' constraints are becoming more apparent given the constantly morphing landscape of cyber threats. The intricacies and interdependencies within cyberspace extend beyond borders, posing challenges for state-centred measures to adapt to the evolving terrain [22].

Additionally, state-centric approaches may struggle to address cyber threats originating beyond their borders, hindering their ability to protect national interests effectively [23]. With these limitations, there is a growing need for broader, more inclusive approaches to cybersecurity governance. Exploring multi-stakeholder models that involve government agencies, businesses, and civil society organisations can foster collaboration and leverage diverse expertise, ultimately leading to more robust and adaptable cybersecurity strategies [3].

Likewise, strengthening public–private sector collaboration can facilitate information sharing and coordinated action to combat cross-border threats [24]. For instance, the Australian government's partnership with academic researchers exemplifies the shift towards collaborative governance models, acknowledging the complexity of contemporary cyber challenges [25]. By incorporating a wider range of perspectives and experiences, such collaborative approaches can enhance the effectiveness and adaptability of cybersecurity strategies in addressing evolving threats.

Addressing the complexities of contemporary cyber threats necessitates moving beyond state-centric approaches and embracing collaborative and inclusive governance models that incorporate a more comprehensive range of stakeholders and expertise.

3.3. The Rise of Non-State Actors in Cybersecurity

The role of non-state actors in cybersecurity is changing significantly. These actors, including international NGOs, private sector organisations, and civil society groups, are playing a role alongside state actors in addressing the challenges of the digital age. Their role is critical in navigating the evolving cybersecurity threats landscape.

Non-state actors are actively involved in cybersecurity governance models. They partake in initiatives to build capacity by offering training and resources to government agencies and stakeholders on practices and emerging threats. Moreover, they engage in advocacy work to influence policymaking and raise awareness about important ICT security issues [1]. This collaborative approach encourages sharing knowledge and expertise, resulting in more robust and adaptable cybersecurity strategies. They are crucial in safeguarding critical national infrastructure from ever-present cyber threats. Their knowledge, tools, and creative methods complement the government's actions in ensuring that systems are strong. Their collaboration with government bodies and partners helps create cybersecurity strategies to deal with weaknesses in infrastructure sectors. This joint work plays a role in upholding the operation and safety of services that are important to society.

In today's conflicts, groups use strategies and tactics to achieve their objectives. Petrosyan [26] analysed how non-state actors are involved in warfare, focusing on conflicts such as those in Syria and Nagorno Karabakh. Their research highlights how non-state actors strategically use cyberspace to disrupt enemy operations, spread propaganda, and coordinate strikes quickly and accurately. Non-state actors undermine traditional state-centric conflict resolution and security governance by utilising cyberspace as a battleground, which presents distinctive obstacles to international stability and peacekeeping endeavours. Furthermore, their ability to take advantage of technological weaknesses and participate in information warfare hinders efforts to effectively prevent and counter their actions [27].

Overall, the rise of non-state actors in ICT cybersecurity represents a significant shift in the global security landscape. Their diverse contributions shape policy, infrastructure protection strategies, and responses to cyber warfare. As the digital age continues to evolve, effective collaboration between state and non-state actors will be crucial for building a secure and resilient ICT ecosystem.

3.4. Contributions of Non-State Actors to Cybersecurity

Non-state actors are crucial in strengthening cybersecurity resilience by shaping global norms and standards, fostering knowledge transfer, and collaborating on joint initiatives. Non-state actors significantly influence cybersecurity norms in the digital age [28]. They actively participate in multi-stakeholder dialogues and advocacy campaigns, contributing diverse perspectives to developing best practices and governance frameworks. This collaborative approach leads to more comprehensive and effective cybersecurity policies. Furthermore, non-state actors leverage their expertise and connections to raise awareness and encourage compliance with these standards. This fosters a culture of accountability and collaboration among all stakeholders, including governments, businesses, and individuals [4].

At the national and regional levels, capacity-building initiatives play a major role in enhancing cybersecurity expertise. Non-state actors, such as international NGOs and civil society organisations, actively contribute to these efforts by organising training programmes and promoting knowledge exchange [29]. This equips stakeholders with the necessary skills and resources to effectively address the evolving threats in cyberspace.

Non-state actors play a crucial role in forging partnerships, exchanging insights, and shaping norms. Their skills and connections enable them to work with governments and international organisations on initiatives to strengthen cybersecurity and promote cooperation against cyber threats [5]. This collaborative approach involves diverse entities such as industry associations, academic institutions, and think tanks partnering with stakeholders to enhance cybersecurity practices and foster collaboration. These efforts enhance defence capabilities on a global scale by leveraging resources and networks to share

expertise and intelligence. Engagement in these initiatives promotes trust and resilience across sectors and boundaries. Enhancing cooperation among parties and joint actions is crucial in addressing cyber risks and creating a safer online environment for all.

Case studies provide valuable insights into the specific measures and collaborations carried out by non-governmental groups to tackle distinct cyber dangers and difficulties effectively. Maschmeyer [30] explores how non-state players undermine cyber operations and wield structural influence in global politics. Non-state actors impact cybersecurity policy development and question the prevailing narratives on a global scale through strategic partnerships and lobbying efforts. Studying these case studies can help policymakers and cybersecurity experts understand the techniques used by non-state actors to reduce cyber dangers and enhance cybersecurity.

These findings can guide the creation of policies and programmes that utilise the assets and talents of non-state actors to improve cybersecurity resilience and promote international cooperation. The in-depth research on state-sponsored cyberattacks that was conducted by Azubuike [31], clarifies the complex relationships between governing bodies and non-governmental organisations when it comes to mitigating cyber threats. Non-state actors are crucial in helping government entities and private sector organisations reduce cyber risks and improve cyber resilience by offering expertise and technological assistance. Figure 3 illustrates the roles of example state and non-state actors in cybersecurity governance.

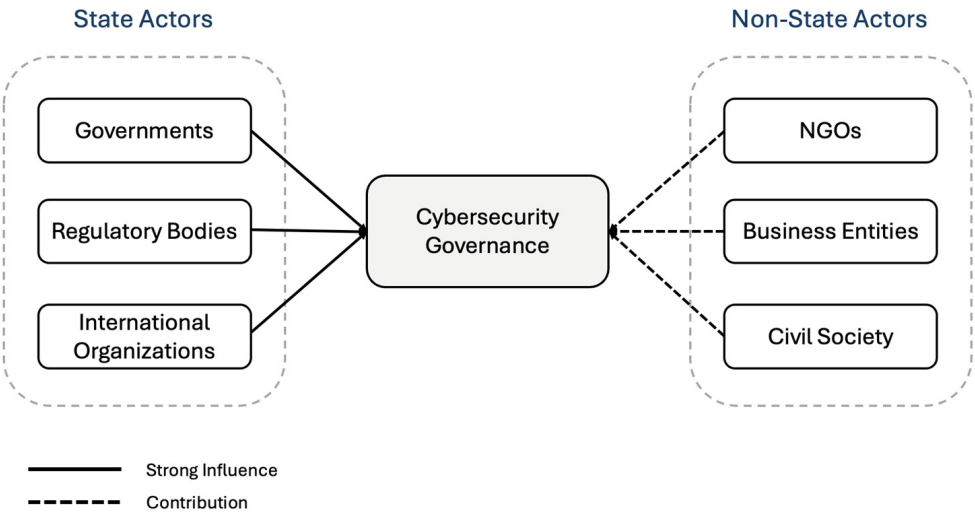

Figure 3. Roles of state and non-state actors in cybersecurity governance.

3.5. Challenges Faced by Non-State Actors

Non-state players have impacts on cybersecurity and face obstacles that can affect their ability to deal with cyber threats efficiently. Limited resources are a major challenge for these stakeholders when they are involved in cybersecurity initiatives. Maulana and Fajar [32] explore cyber diplomacy and its barriers in the society era. They shed light on state and non-state actors' challenges, including various threats (e.g., political process and privacy). There are also other challenges mentioned in other studies, such as limited expertise and constrained technical capabilities [33]. These barriers prevent these entities from establishing strong cybersecurity measures and responding promptly to cyber threats. For example, inadequate resources can hinder their capacity for research, designing solutions, and addressing cyber threats, which restricts their role in strengthening cybersecurity resilience. Adapting to changes in the cyber threat landscape and building partnerships with governments, businesses, and other entities and communities can be difficult for non-state actors due to limited resources. Thus, resource allocation is essential for enhancing non-state players' role and efficiency in cybersecurity and cyberspace resilience.

Legal barriers pose challenges for organisations involved in addressing cybersecurity threats. Abdullahi and Musa [34] emphasised the hurdles faced by non-state entities in

navigating the legal landscape. These actors deal with uncertainties and jurisdictional issues when combating cybercrimes, which hinders their ability to uphold cybersecurity norms effectively [35]. The absence of frameworks and the complex nature of cross-border cyber incidents worsen challenges. Non-state actors struggle to hold cybercriminals accountable, underscoring the importance of legal expertise and global collaboration.

Lewis and Baez [36] study theories related to control and how they influence warfare, underlining the difficulties in coordinating responses to cyberattacks that involve stakeholders such as government, agencies, businesses, and organisations. The lack of coordination among these groups arises from conflicts of interest, disparities in knowledge levels, and conflicting objectives. Consequently, this results in disjointed and chaotic responses to cyber threats, diminishing the overall effectiveness of cybersecurity measures. Overcoming coordination challenges requires improving communication mechanisms, establishing avenues for collaboration, and promoting trust among stakeholders within the cybersecurity community. Addressing these challenges can enhance the ability of non-state actors to respond to cyber threats effectively, strengthening cybersecurity governance and resilience on a global scale.

The continuously evolving landscape of cyber threats adds another layer of challenge for addressing cybersecurity issues. Diro, Kaisar [37] explained anomaly detection within information networks, underscoring the agility of threats and the importance of adaptable cybersecurity methods in response to evolving threats. Non-state entities must accommodate new cyber threats and vulnerabilities, necessitating ongoing investment in research, development, and capacity-building efforts to stay ahead of cyber attackers. Taking a proactive and adaptable stand for those outside government circles can proactively predict and respond to emerging threats in cyberspace.

3.6. Impact of Non-State Actors in the Cybersecurity Landscape

Non-state actors significantly affect the cybersecurity norms and policies that are vital in mitigating cyber threats. Through avenues such as advocacy, research, and engagement with diverse stakeholders, they substantially impact cybersecurity standards and regulations. For instance, Painter [38] examines how non-state actors, including industry companies, civil society organisations, and academic institutions, collaborate to shape cybersecurity legislation, particularly through multi-stakeholder participation in cyber stability issues within the United States. These actors are instrumental in influencing cybersecurity norms and standards by facilitating discussions among stakeholders from various sectors, thus enabling the consideration of a broad spectrum of viewpoints and interests. Consequently, they contribute to developing inclusive and representative cybersecurity governance frameworks that address cyber threats' complex and evolving nature through collaborative efforts.

Additionally, non-state actors are crucial in enhancing the legitimacy and rationale of cybersecurity governance by actively participating in deliberative processes and decision-making procedures. Zhao [39] explores how legitimacy is conferred through discussions involving non-state actors, focusing on the involvement of women's groups in the United Nations Framework Convention on Climate Change. Advocacy groups and grassroots organisations, among other non-state actors, contribute diverse perspectives and expertise to policy dialogues, enriching the deliberative process and fostering inclusive and representative cybersecurity governance frameworks. Their involvement ensures that a wide array of viewpoints is considered, resulting in more robust and comprehensive cybersecurity policies that address the requirements and concerns of various stakeholders.

Nonetheless, regulatory cybersecurity governance encounters challenges in establishing credibility, as non-state players struggle to assert their influence on developing regulatory frameworks and standards. Dunn Cavelty and Smeets [40] examine the evolution of regulatory cybersecurity governance, focusing on establishing the European Union Agency for Cybersecurity (ENISA) and its challenges in acquiring accurate information. Industry stakeholders and cybersecurity specialists seek to garner credibility and influ-

ence in shaping cybersecurity policies. However, they face resistance from entrenched state-centric governance paradigms that often prioritise traditional governmental structures and decision-making processes. Despite these challenges, non-state actors persist in enhancing cyber governance by advocating for inclusive and participatory approaches that acknowledge their diverse viewpoints and expertise.

Non-state actors are pivotal in bolstering cybersecurity resilience by establishing new governance structures and implementing capacity-building programmes, notwithstanding their challenges. They contribute to developing flexible and robust cybersecurity strategies by fostering collaboration and facilitating information sharing among stakeholders [41]. These initiatives effectively mitigate emerging cyber threats and vulnerabilities, ultimately enhancing the overall resilience of cyber defences. Thus, non-state actors influence the cybersecurity landscape considerably, guiding it towards greater agility and responsiveness to evolving threats.

3.7. Enhancing Collaboration Between State and Non-State Actors

Collaboration between governmental and non-governmental entities is pivotal for effectively addressing the intricate and evolving challenges of cybersecurity. It facilitates sharing information, resources, and knowledge, thereby significantly enhancing cybersecurity resilience [42]. Governments, corporate sector organisations, and civil society groups can develop innovative solutions to combat changing cyber threats by pooling their resources and expertise. Collaborative projects foster trust and cooperation among stakeholders, which is essential for developing robust cybersecurity frameworks. Moreover, they empower the cybersecurity community to anticipate emerging threats and protect digital infrastructure by leveraging multiple stakeholders' combined insights and capabilities. State and non-state entities possess distinct capacities that, when combined, can effectively address cybersecurity issues.

Insurance companies have an important role in motivating businesses to invest in cybersecurity [43]. They do this by working with governmental regulators, providing incentives and expertise for risk assessments, and mitigating risks. Through these partnerships, a strategy is developed to take advantage of strengths in order to address cybersecurity challenges efficiently. Involvement also prompts organisations to proactively manage cyber risks by implementing robust cybersecurity measures to protect themselves against cyberattacks. The collaboration between public and private sector partners, including insurers, is crucial in building a landscape that can effectively and proactively respond to cyber threats [44].

Policymakers should prioritise the establishment of multi-stakeholder forums and partnerships to improve coordination between governmental and non-governmental entities in cybersecurity. These forums provide a formal platform for stakeholders from different sectors to exchange ideas, share insights, and combine resources [45]. They facilitate open communication and collaboration among various parties to address shared cybersecurity issues and develop joint solutions. Moreover, these platforms help exchange best practices and lessons learned, enhancing cybersecurity resilience across various sectors and businesses. Policymakers are instrumental in promoting cooperation between governmental and non-governmental entities through legislative frameworks and funding mechanisms. Additionally, policymakers may promote the creation of new cybersecurity solutions by investing in joint research projects, capacity-building programmes, and knowledge-sharing activities.

Enhancing capacity is crucial for fostering cybersecurity collaboration between governmental and non-governmental organisations [46]. Iacono and Mastroianni [47] proposed a modelling framework that can be used by governments to create and evaluate policies to make the cyber environment safer for users. Their work can help policymakers make policies and regulations effective in reducing privacy and security risks. Training programmes, workshops, and knowledge exchange initiatives can help foster teamwork and encourage a culture of cooperation in addressing cyber threats. Investing in capacity-building projects

enables stakeholders to improve their comprehension of cybersecurity threats and acquire the necessary skills and experience to address cyber issues proficiently. These projects offer opportunities for stakeholders to exchange knowledge, share best practices, and collaborate on methods to tackle shared cybersecurity issues. Capacity building enhances trust and confidence among stakeholders, promoting stronger interactions and partnerships in the cybersecurity ecosystem. It is crucial for enhancing collaboration and bolstering the collective resilience of governmental and non-governmental organisations against cyberattacks.

3.8. Technological Solutions and Innovations

The increase in cyber threats today is due to our dependence on technology. This section focuses on understanding the concept of cyber resilience, leveraging advanced tools such as artificial intelligence (AI), blockchain, and Internet of Things (IoT) security.

Integrating AI and blockchain technologies into security frameworks has sparked interest among researchers. For example, Girdhar, Singh [48], examined the use of AI and blockchain in enhancing security for cyber-physical systems. Similarly, Tyagi [49] explored how blockchain and AI technologies contribute to securing the Internet of Things and industrial Internet of Things applications. These studies shed light on innovative approaches to combating cyber threats and demonstrate the potential of these technologies in fortifying cyber resilience.

The rise in the use of IoT devices represents a turning point in technology, presenting a mix of challenges and opportunities. The increase in connected devices, especially in areas like homes, wearable technology, industrial equipment, and infrastructure, elevates the risk of cyberattacks, as noted by Lone, Mustajab [50]. In their study, Lone et al. conducted a deeper analysis of the security challenges within the realm of IoT. Their findings emphasise the importance of implementing strong security measures to protect IoT environments from cyber threats, underscoring the urgency of implementing proactive defence mechanisms. Moreover, their research highlights the vulnerabilities found in IoT setups, emphasising the significance of robust security measures in developing and deploying IoT solutions. As the network of connected devices expands, bad actors will find more opportunities to breach systems. This study underscores the importance of emphasising cybersecurity in IoT implementations by proactively detecting and addressing vulnerabilities to predict and prevent security breaches. It stresses the need for stakeholders across industries to take precautionary steps.

In the domain of global cybersecurity governance, the increase in advanced technologies such as Artificial Intelligence (AI), blockchain, and the Internet of Things (IoT) introduces distinctive risks and regulatory challenges. The integration of AI in cyber threats presents a multifaceted challenge due to the emergence of sophisticated AI-driven cyberattacks and data manipulation by creating deepfake content. Regulatory challenges are particularly evident in the standardisation of AI in cybersecurity and necessitate a comprehensive approach to address ethical considerations and harmonise regulations across international boundaries [51,52].

Meanwhile, blockchain technology introduces decentralised threat vectors and fosters anonymity, promoting illegal activities and posing potential cybersecurity risks. Regulatory challenges for blockchain pertain to the need for global harmonisation of regulations and the establishment of interoperable standards to address diverse implementations and interpretations. Furthermore, the widespread adoption of IoT devices significantly expands the attack surface. It raises data privacy and integrity concerns, calling for standardised regulations and governance practices to mitigate fragmented security frameworks and complex supply chain oversight [50,53].

In navigating these challenges within global cybersecurity governance, collaborative efforts are imperative to formulate interdisciplinary regulatory frameworks that effectively address the technical intricacies of AI, blockchain, and IoT, thus safeguarding against emerging cyber threats. It is essential for state and non-state actors to work collectively in establishing adaptive governance mechanisms that accommodate the evolving nature

of cybersecurity risks in the digital age, promoting harmonisation of regulations and cybersecurity best practices to foster resilience and address the complexities posed by these technologies at a global scale.

To enhance cyber resilience, particularly during an ever-evolving cyber threat landscape, Vegesna [54] dives into an analysis of cyber resilience focusing on the effectiveness of AI-based threat detection and mitigation systems. By strengthening their cyber defence capabilities, organisations can rapidly detect and neutralise emerging threats using AI algorithms. AI's capability to adjust and learn from patterns in data and threat landscapes enhances cyber defences and thwarts potential breaches. Saeed, Altamimi [55] suggest a structured approach for managing cyber threats, underscoring the importance of proactive defence tactics in mitigating cyber risks. Their strategy introduces a systematic framework for fortifying cyber defences and streamlining responses to cyber incidents effectively. Leveraging AI-powered solutions for threat detection and mitigation is crucial in addressing cyber risks, protecting assets, and ensuring business continuity in the face of evolving threats.

When it comes to the cyber challenges faced by entities, including state-owned businesses, a thorough examination of the challenges related to their digital transformation is essential. Saeed, Altamimi [55] described the obstacles organisations face during this process. State-owned businesses are prone to a range of security gaps and threats arising from factors like outdated systems and sophisticated cyberattacks launched by malicious actors aiming to exploit weaknesses in digital infrastructure. The study emphasises the necessity of developing robust security measures tailored to state-owned entities' specific needs and challenges. A comprehensive strategy involves addressing advancements in technology preparedness at the organisational level and regulatory requirements.

Advanced cybersecurity tools such as AI-driven threat detection systems and blockchain-strengthened security measures are vital in fortifying defences and enhancing resilience against emerging threats. Safitra, Lubis [56] underscore the importance of training programs, awareness campaigns, and incident response protocols to boost defences and instil a culture of cyber awareness in government-controlled entities. Establishing robust regulations is critical for defining standards and ensuring compliance levels in state-owned entities. Organisations can reduce cyber risks, enhance resilience, and confidently navigate the digital landscape by enforcing directives covering these aspects.

Table 3 lists publications categorised according to their relevance and impact within the subject areas. Each publication is grouped based on its significance in discussing key topics, providing evidence, and sharing concepts.

Table 3. Publication categories and description.

Reference	Category	Methodology	Correlation to Study
[34]	Cybersecurity (Legislation)	Qualitative analysis of legal frameworks and case studies.	This paper investigates non-state actors' legal uncertainty and jurisdictional challenges when dealing with cybercrimes, emphasising the need for stronger legal institutions to manage cybersecurity. They also explained the effects of emerging issues like "cybersecurity, climate change, evolving nature of the international law", which might make the legitimacy of international law challenging. The paper suggests the importance of having a structure in the international arena. It sees international law as a result of decisions made collectively by states who choose to adhere to agreed rules.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[9,18,53,54]	Cybersecurity (Threat Detection)	Case study and statistical analysis	The papers propose novel cybersecurity prediction techniques that forecast potential attack methods against critical infrastructure (CI) systems, depending on specific CI and attacker motivations. Their approach uses improved machine learning models to predict potential cyberattacks against CI systems. They highlight that predicting cyberattacks can help CI security teams better defend and protect their systems, conduct urgent cybersecurity awareness and training, and match the needs of new project plans and budgets.
[53,54]			These studies investigate threats in cyberspace and their implications, for instance for national security policy and the healthcare sector. The studies explored the efficacy of AI models and technologies in fortifying cyber defences (e.g., for IoT) by enabling proactive threat identification and response mechanisms. They also evaluate the resilience of AI-integrated systems in dynamically adapting to the constantly mutating nature of cyber threats.
[57]	Cybersecurity	Case studies and survey analysis (Literature review)	Offers valuable perspectives on the ability of industrial networks to withstand cyberattacks, focusing on the difficulties and approaches to strengthening cybersecurity in vital infrastructure. This study identifies the main technical and human-related challenges, practical limitations, and current cyber resilience needs of industrial networks, particularly focusing on industrial control systems (ICSs) and industrial Internet of Things (IoT).
[6]	Alliance Building	Literature review and comparative analysis	The study pinpoints the objectives of public–private partnerships (PPPs) in building critical infrastructure resilience (CIR) by analysing 12 selected publications and 10 governmental and institutional reports. It highlights the limited research attention dedicated to the concept of PPP in CIR despite its recognition as a mechanism for building CIR.
[46]	Analysis	Neorealist analysis and statistical modelling	The research delves into how cyberspace's ancient security problem is linked to neorealist theory. It suggests that the absence of clear lines and attribution in the cyber realm heightens the security problem. States' actions to boost their cybersecurity can unintentionally jeopardise others, fuelling a race in cyber capabilities. The study highlights the challenges of establishing mutual security in cyberspace, given the mistrust and the secretive aspect of cyber operations.
[14,19]	Cybersecurity	Literature review and qualitative analysis	The studies emphasise how countries adjust their military policies and tactics to deal with cybersecurity threats, acknowledging cyberspace as a crucial battleground where the lines between war and peace are increasingly blurred. It stresses the importance of cooperation in navigating the challenges of cyber warfare effectively. The research also highlights the importance of global cooperation in countering the growing dangers of malicious software by promoting sophisticated defence strategies. Overall, these findings underscore the crucial role of united responses to address the impacts of cyber threats, in a world.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[20]	Cybersecurity	Case study approach and qualitative analysis	The study advocates for an international commitment to crafting and executing cybersecurity strategies using cutting-edge technologies to minimise the impacts of such threats. It stresses the importance of countries working together and taking proactive measures at the state level to tackle the increasing challenges posed by cybersecurity.
[31]	Cybersecurity (Strategy and Diplomacy)	Case study analysis and interviews	The research looks into how state cyberattacks have evolved into a key weapon in conflicts, with countries turning to cyber activities more and more to reach their goals. It underscores the importance of coordination among countries and setting standards and treaties to reduce the dangers and potential for escalation of these cyber dangers on a worldwide scale.
[4]	Cybersecurity	Statistical and case studies analysis	The article examines how the EU and the US engage in cyber diplomacy, with the EU emphasising cooperation and normative structures, while the US focuses on alliances and defence capabilities. It underscores the importance of collaboration across the Atlantic to tackle the consequences of cyber threats, proposing that aligning these strategies may boost cyber governance and resilience on a scale.
[43]	Cyber Insurance Challenges	Review of existing industry reports and academic research	The research highlights how cyber insurance is now being seen as a way to encourage improved cybersecurity practices among businesses, which could help minimise the effects of cyberattacks. It proposes that cyber insurance and government strategies can contribute significantly to promoting collaboration and strengthening the worldwide cybersecurity environment by linking financial incentives with increased security precautions.
[37]	Cybersecurity (Anomaly Detection)	Survey analysis and comparative study	Examines the ever-changing nature of cyber threats and emphasises the need for adaptable cybersecurity strategies, underscoring the necessity for non-state entities to adjust and innovate to effectively face emerging cyber risks. It stresses the importance of collaborating internationally to enhance detection methods. Given the dependence on space assets worldwide, they have become prime targets in today's era of digital warfare. This has far-reaching consequences for security at both the national and global levels.
[40]	Cybersecurity (Regulatory Governance)	Interviews and policy analysis	Explores non-state actors' challenges in influencing regulatory cybersecurity governance, emphasising state-centric opposition and the need for inclusive policymaking. The research explores the challenges faced by the European Union Agency for Cybersecurity (ENISA) in establishing itself as a leading authority in cybersecurity governance within the EU. It underscores the significance of boosting ENISA's influence and funding to promote stronger state responses and cooperation, which are critical factors in tackling cybersecurity challenges in the era.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[15]	Cybersecurity	Qualitative analysis and case studies	The study examines how states' development and deployment of offensive cyber capabilities can escalate conflicts and increase the likelihood of state-sponsored cyberattacks. It argues that international cooperation and the establishment of norms to regulate the use of offensive cyber operations are urgently needed to mitigate these risks and prevent their potential to destabilise global security.
[27]	Cybersecurity (Legislation)	Legal analysis and case studies	The article explores the legal challenges of holding non-state actors accountable for war crimes committed in cyberspace under the International Criminal Court (ICC) framework to address the complexities of detecting and prosecuting cybercriminals to uphold in the warfare landscape.
[42,48,49]	Cybersecurity (Technological Solutions)	Experimental studies and qualitative analysis.	The papers collectively highlight the dual role of emerging technologies like AI, IoT, blockchains, and quantum computing in both enhancing cybersecurity and introducing new risks, emphasising the need for proactive cyber diplomacy to manage these challenges. They encourage collaboration to establish frameworks and standards that harness AI and blockchain technology to boost security for systems in the domains of the IoT and industrial IoT. Additionally, they tackle the security issues posed by these technologies in the landscape of digital warfare.
[1]	Advocacy	Survey analysis and literature review	The study points out that cybersecurity governance calls for asking states, private sector players, and society to join hands in diplomatic initiatives aimed at establishing an international cybersecurity framework. It underscores the importance of cooperation and open communication in tackling the ever-changing nature of cybersecurity risks in the age of digital warfare to create a secure and robust cyber space.
[12,13]	Cybersecurity	Literature review and case studies	They explain advanced persistent threats (APTs) and their persistence, complexity, and network strategy. The articles underscore how cyber threats, such as ransomware attacks and supply chain weaknesses, are evolving quickly and becoming more complex. These threats raise serious concerns for security and underscore the importance of prompt action and collaboration among nations to create strategies and frameworks capable of dealing with these emerging challenges.
[36]	Cybersecurity (Coordination Study)	Case study analysis and surveys	This study investigates non-state actors' coordination challenges in combating cyberattacks, focusing on conflicting interests and the need for better communication and trust to strengthen cybersecurity efforts. The study examines the ways in which geopolitical and economic aspects influence state behaviours in cyber warfare control theory to analyse these dynamics. The study emphasises the importance of comprehending these factors in order to develop state strategies and promote cooperation. These actors play a role in shaping the responses and policies required to tackle the challenges posed by cybersecurity threats in today's era of digital warfare.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[24]	Cybersecurity (Capacity Building)	Case studies and interviews	The research looks at how big companies, such as Microsoft, are influencing cybersecurity measures. It emphasises the importance of collaborations between the public and private sectors in shaping cybersecurity policies and dealing with cybersecurity issues. It stresses the significance of enhanced international cooperation and united governmental efforts to tackle the challenges posed by threats in today's digital landscape, where the sector's role is growing.
[23]	Cybersecurity (Diplomacy)	Literature review and case studies	The research examines how the US has been turning to soft power in its cyber diplomacy efforts to shape global cybersecurity norms and encourage cooperation. It points out that navigating the landscape of digital conflict calls for utilising soft power to forge partnerships, inspire trust, and create a joint cybersecurity framework to tackle new threats.
[3]	Policy Development	Literature review and policy analysis, comparative study	The research paper highlights that Chinese multi-stakeholder cybersecurity governance emphasises state-centric control, while incorporating various actors to manage threats. Nevertheless, it faces challenges in balancing national authority with international cooperation. Also, it underscores the need for a reformed international cybersecurity regime that accommodates various governance models and effectively enhances collaborative efforts to address the global nature of cyber threats.
[50]	Cybersecurity	Surveys and case studies	Examining non-state actors' coordination challenges in cyberattack resolution, highlighting the need for better communication and trust to improve cybersecurity. The research shows that the increase in IoT devices escalates cybersecurity issues because of their vulnerabilities and the challenge of securing connected systems. It points out ways to strengthen security by implementing standards, encryption methods, and improved incident response plans, underscoring the importance of cooperation among stakeholders in tackling these emerging threats.
[28,38]	Cybersecurity (Norm Development)	Surveys and interviews	Explores how non-state actors influence cybersecurity norms and governance frameworks, emphasising the importance of cooperation in promoting accountability and adherence. The first research paper [28] explores the evolution of cybersecurity norms, showing a shift towards structured frameworks as countries and global organisations focus more on cybersecurity in light of growing digital threats. The second paper [38] talks about the influence of US engagement in shaping cybersecurity stability on a global scale and underlines the significance of diverse viewpoints in boosting collaborative defence mechanisms and strengthening cybersecurity frameworks.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[30]	Cybersecurity (Strategy and Diplomacy)	Case study analysis and interviews	The study delves into how cyber operations are employed as a means of subversion, enabling states to exert influence by undermining the foundations of other nations through means of warfare. This article combines intelligence scholarship with international relations theory to create a novel theory of subversion as a form of reverse structural power. It emphasises how this power shift disrupts responses while underscoring the importance of international cooperation and standards in addressing the destabilising impacts of cyber risks within geopolitics.
[32]	Cybersecurity (Strategy and Diplomacy)	Qualitative analysis and survey	The study underlines that cyber diplomacy is becoming increasingly crucial in addressing the complex cybersecurity challenges, as it facilitates international cooperation and conflict resolution in the digital era. However, it also identifies significant challenges, such as differing national interests, legal frameworks, and the rapid growth of technological change, which complicate the development of effective global cyber policies.
[58]	Cybersecurity (Policy Development)	Policy analysis and theoretical framework	The document suggests a flexible cybersecurity governance system that aims to boost resilience against changing cyber threats by integrating real-time data analysis, cooperation among stakeholders, and ongoing policy adjustments. It emphasises the need for governance frameworks that can swiftly respond to challenges and promote collaboration to mitigate global cybersecurity risks effectively.
[7]	Cybersecurity	Literature review and case studies (textbook)	The authors highlight that state responses to cybersecurity threats in the digital warfare era increasingly underline the development of robust cyber defence strategies and international partnerships. The book stresses the necessity of global cooperation, including establishing norms and frameworks, to counter the escalating risks posed by cyber threats effectively. This also mitigates the potential ramifications of cyber warfare on national and international security.
[59]	Cybersecurity (Cognitive Analysis)	Experimental studies and qualitative analysis	Examines cognitive biases in cybersecurity research and analysis, emphasising the need to address institutional constraints and biases to develop effective cybersecurity approaches. The study shows that state reactions to cyber dangers are usually responsive and depend on how attacks are discovered, which affects their views of threat landscapes. This bias underscores the importance of enhancing global collaboration and sharing efforts to create cybersecurity strategies and gain insight into the extent and impacts of cyber threats in the age of digital warfare.
[26]	Cyber Warfare Strategies	Case studies	The study indicates that non-state actors problematise state responses to cybersecurity threats, as they often exploit digital warfare tools outside traditional state control. It underscores the significance of cooperation in handling the cybersecurity challenges posed by these entities. Their involvement in conflicts like those in Syria and Nagorno-Karabakh highlights the need for coordinated global initiatives to reduce the effects of cyber threats.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[21,56]	Cybersecurity (Mitigation Strategy)	Literature review and case studies	Investigates the impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. The first study [21] emphasises the increasing vulnerability of critical infrastructure to cyber threats and calls for governmental actions to prioritise enhancing safeguarding measures and international collaboration to defend these crucial systems. The second study [56] endorses a proactive approach, suggesting that state-led countermeasures and global cooperative frameworks are essential to mitigate the risks of cyber warfare in the digital era.
[55]	Cybersecurity (Businesses and State-Owned Firms)	Case studies and literature review	This study shows that digital transformation (DT) increases efficiency and productivity but presents new challenges related to cybersecurity risks, such as data breaches and cyberattacks. The paper emphasises the importance of a comprehensive knowledge of cybersecurity threats during DT implementation to prevent interruptions due to malicious activities or unauthorised access. The article highlights that state responses to digital warfare must involve robust cybersecurity policies and international cooperation to address the increasing complexities of cybersecurity threats. It emphasises that coordinated global efforts and shared cybersecurity frameworks are crucial for enhancing business resilience against cyberattacks in the digital era.
[25]	Cybersecurity (Legislation)	Legal analysis and case studies	The main point of the article is that there is a limited treatment of intelligence by IR and strategic studies academics in Australia. This impacts research outcomes and public comprehension of policymaking in Canberra. It stresses the importance of increasing academic attention towards understanding the role and value of intelligence in Australia's foreign and defence policies. This study discusses how state responses in the digital warfare era require enhanced intelligence-sharing and international cooperation to counter cybersecurity threats effectively.
[60]	Cybersecurity (Machine Learning)	Literature review and case study	The article emphasises the need to incorporate advanced machine learning algorithms to detect and prevent cyberattacks effectively during digital warfare. It underscores the significance of countries collaborating to share technological advancements and data to improve overall cybersecurity defences.
[29,41]	Capacity Building	Case studies and survey analysis	The studies stress the importance of international legal frameworks and supranational governance structures to respond to cybersecurity threats in the digital age. They underscore how cooperation guided by legal standards and security capabilities can help tackle the security issues caused by technology worldwide.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[22]	Policy Development	Policy analysis and literature review	The study sheds light on how Norway's counterterrorism strategies in the digital age aim to remove politics from violence by using a state-centred and personalised approach to tackling cybersecurity challenges. It emphasises the importance of working together internationally and coordinating actions to deal with the wide-ranging effects of cybersecurity in counterterrorism, underscoring the significance of grasping the complexities of violence in global cybersecurity strategies.
[5]	Cybersecurity (Strategy and diplomacy)	Case studies and comparative analysis	The article emphasises how leading countries like the United States, China, Russia, and France and the European Union increasingly see and deploy multi-stakeholder cyber diplomacy (MCD) efforts as tools to advance their own pursuits. The article highlights the importance of effectively addressing challenges in the era by advocating cyber diplomacy. In this strategy, governments, companies, and civil society collaborate to shape norms, stressing the significance of working together and reviewing national approaches, which are crucial for establishing a robust cybersecurity system to address cyber risks.
[2]	Policy Development	Survey analysis and case studies	Examines how non-state actors shape informal governance structures in the global cybersecurity environment, emphasising their influence on policymaking and innovation. The article claims that the international cybersecurity regime is characterised by pervasive informality, where non-state actors and informal diplomatic channels play a significant role in shaping responses to cyber threats. It emphasises that state responses and international cooperation must adapt to this informality by engaging various actors and leveraging flexible diplomatic approaches to effectively manage the geopolitical complexities of cybersecurity in the digital warfare era.
[17]	Cybersecurity	Qualitative case study	The article emphasises that providing employees with cybersecurity training plays a vital state response role in mitigating the threats of spear phishing, identity theft, and ransomware attacks during warfare. It also emphasises the significance of international collaboration to create guidelines and best practices for training programs that can strengthen global resilience against cybersecurity threats.
[61]	Norm Development	Policy analysis and case studies	The article highlights the significance of building multi-stakeholder structures that include governments, the private sector, and civil society to establish cybersecurity norms in the age of digital warfare. It stresses the need for cooperation and exchanging insights from past incidents when developing solid cybersecurity frameworks to address growing threats.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[16]	Cybersecurity (Legislation)	Legal analysis and case studies	This article focuses on the challenge of interpreting Article 2(4) of the UN Charter in the context of warfare, such as cyberattacks. The paper highlights the complexities in determining what qualifies as the "use of force" in cyber warfare. It underscores the significance of establishing a legal framework for categorising cyberattacks and shaping how states respond. It also underscores the difficulties and ambiguity in applying traditional laws to cyberattacks utilising advanced technologies.
[35]	Cybersecurity (Legislation)	Legal analysis and case studies	Explores navigating the cyber legal landscape and protecting legal entities through comprehensive cybersecurity strategies. The article emphasises that state responses in the digital warfare era should include comprehensive cybersecurity strategies tailored to protect legal entities from evolving cyber threats. It also looks at how AI is being used in global dispute resolution and touches on how blockchain technology enhances legal protections in the digital economy.
[62]	Cybersecurity (Mitigation Strategy)	Literature review	The article underlines the importance of Artificial Intelligence (AI) in strengthening state defences against cybersecurity risks by providing cutting-edge technologies for detecting and responding to threats in the age of warfare. It also underscores the importance of collaborative efforts in researching AI and setting up worldwide norms to tackle the complex and evolving challenges caused by cyber threats.
[7]	Cybersecurity (Strategy and Diplomacy)	Literature review (textbook)	Discusses politics and strategies in cybersecurity. This textbook comprehensively introduces global cyber conflict, covering its historical, technical, and strategic dimensions. It explains various topics, including the transformation of warfare, diverse views on digital warfare, policies and approaches, challenges in ensuring adherence to international standards, and the influence of technologies such as AI and quantum computing. The book underlines that governments must address threats with an integrated blend of politics in the digital age, underscoring the importance of national cybersecurity frameworks that can adapt. The book underscores the value of across borders as it calls upon joint endeavours to define cybersecurity guidelines and strategies for mitigating the impact of cyber threats more efficiently.
[45]	Norm Development	Policy analysis and case studies	Examines the role of insurers in shaping international cybersecurity norms about cyber war. The argument made is about how insurance companies influence worldwide actions by influencing views on government behaviour in online spaces through their strategies for dealing with the risks and responsibilities arising from cyber activities and warfare. This point is highlighted by discussing the 2017 NotPetya cyberattack, which sparked discussions between insurance providers and policyholders on whether Russia's actions should be considered an act of war. This could result in such incidents falling outside the coverage provided by typical war exclusion clauses.

Table 3. *Cont.*

Reference	Category	Methodology	Correlation to Study
[11]	Cybersecurity	Literature review	Explores the challenges of simulating threats in modern cyber intelligence operations. The research indicates that the significant growth of threat intelligence within the private sector has resulted in a complex environment involving multiple stakeholders, causing various outcomes, such as diminished warning readiness. The dynamics among operational roles advancing attacker skills and deceptive techniques have added layers to cyberattacks, affecting organisations' ability to manage crises.
[39]	Policy Development	Policy analysis and qualitative analysis	Examines non-state actors' roles in policy discussions and decision making to promote cybersecurity governance transparency and inclusivity. This article shows that the rise in cyberattacks has underscored the importance of countries working together to respond effectively to cyber threats. Collaborative strategies and mechanisms are key to tackling the challenges of cyber warfare and security risks/vulnerabilities.

3.9. Emerging Threats in Cybersecurity

Kumar [12] examined the obstacles within the realm of cybersecurity. Kumar's objective is to emphasise the importance of addressing security threats such as APTs, ransomware attacks, vulnerabilities linked to the Internet of Things (IoT), and social engineering tactics. By thoroughly examining and synthesising the available data, the research aims to clarify the nuances of these risks, highlighting their significance for individuals, organisations, and society at large. Kumar stresses the significance of taking action and fostering partnerships to strengthen cybersecurity measures by exploring the complexities. Their work can be a reference point for professional policymakers and researchers within each threat category, providing valuable insights to navigate the challenging landscape of cybersecurity threats today effectively. Table 4 captures cybersecurity threats and their descriptions to help better understand the threats to be mitigated.

Table 4. Threats analysis.

Threat Category	Description
Advanced Persistent Threats (APTs)	Advanced, targeted attacks by nations or groups. Use malware, social engineering, and network exploitation.
Ransomware Attacks	Significant rise targeting all-sized organisations. Data encryption for ransom causes financial loss and service disruption.
IoT Vulnerabilities	Concern over more Internet-connected items. Cybercriminals exploit smart appliance, wearable, and home automation vulnerabilities.
Social Engineering	Trick people into giving crucial information. Emails, calls, impersonation, and pretexting are prominent phishing methods.

Kumar [12] provides insight into the changing nature of digital threats by emphasising the urgent requirement for proactive cybersecurity measures by recognising and analysing emerging threats such as APTs, ransomware, IoT vulnerabilities, and social engineering tactics. Organisations and cybersecurity experts should take note of these findings, which emphasise the significance of implementing a comprehensive defence strategy. This strategy should include strong security regulations, frequent cybersecurity awareness training, and continuous threat intelligence. It is recommended that policymakers prioritise cybersecurity

activities, promoting cooperation among governments, organisations, and individuals to create efficient strategies and structures for sharing information.

Nevertheless, Kumar's research has limitations, including the possibility of bias in threat selection or dependence on obsolete data. Future research should further examine the other factors (e.g., socio-political and psychological factors) that drive cyber threats, investigate new methods of attack in developing technologies, and evaluate the effectiveness of present measures for preventing and mitigating cyberattacks in real-world situations. By engaging in ongoing research and fostering collaboration, cybersecurity communities can effectively enhance their ability to respond to the constantly evolving nature of digital warfare.

Moreover, their study has important implications for guiding the execution of cybersecurity measures in our research on the "Geopolitical Ramifications of Cybersecurity Threats." To comprehensively examine the role of non-state entities in promoting international cooperation and enhancing global cyber resilience, it is crucial to have a thorough grasp of the range of cyber threats. Kumar's categorisation of many types of cyber risks and threats offers a fundamental comprehension of the difficulties for states.

To address these dangers, it is necessary to implement targeted strategies and utilise appropriate technologies. For example, when defending against APTs, it is crucial to implement strategies like network segmentation, advanced threat detection systems, and regular security audits. Ransomware attacks require the implementation of measures such as frequent data backups, thorough employee training on phishing awareness, and robust endpoint security solutions (e.g., endpoint detection and response solutions). To address IoT vulnerabilities, it is important to implement secure device authentication, encrypt data while it is being transmitted, and perform regular firmware upgrades and network segmentation (if needed). To mitigate social engineering threats, it is essential to provide employees with cybersecurity awareness training, implement multi-factor authentication, and conduct regular phishing simulation exercises. Of course, AI-powered solutions can help us to detect, prevent, and respond to all of the mentioned cyber threats.

By aligning these strategies (focusing on non-state actors), we can anticipate how these entities might contribute to implementing and enhancing these measures globally, thereby strengthening global cyber resilience and cooperation in the era of digital warfare. Using a table structure to highlight these mitigation techniques improves clarity. It offers a useful reference for policymakers and stakeholders who want to effectively utilise non-state entities to tackle future cyber dangers. Table 5 presents examples of the mitigation strategies that can be employed to handle all the threats identified.

Table 5. Mitigation strategies.

Threat Category	Mitigation Strategies
Advanced Persistent Threats (APTs)	Segment networks, use advanced threat detection, and audit security.
Ransomware Attacks	Regular data backups, phishing awareness training, and strong endpoint security.
IoT Vulnerabilities	Device authentication, data in transit encryption, firmware updates, and network segmentation.
Social Engineering	Employee cybersecurity training, multi-factor authentication, and phishing simulations.

3.10. Analysis of Non-State Actors in Modern Warfare

Petrosyan [26] analysed the involvement of non-state players in contemporary warfare, offering a complete exploration of the changing dynamics of conflicts. The study highlights the growing significance of non-state actors, such as armed groups and terrorist organisations, in influencing modern battles. Using case studies, Petrosyan demonstrated the emergence of key actors in Syria and Nagorno-Karabakh who exercise influence using both conventional and unconventional strategies. It emphasises the hybrid nature of

their operations, combining superior technical weaponry and artificial-intelligence-driven devices to improve their operational efficacy on the battlefield.

Petrosyan's study enhances our comprehension of the intricate dynamics of contemporary warfare, thereby shedding light on the diverse character of conflicts in today's geopolitical setting. The knowledge obtained from their work emphasises the significance of acknowledging the changing role of non-state actors and their influence on the progress and result of hostilities. This comprehension is essential for policymakers, military strategists, and security professionals responsible for creating efficient tactics to tackle the difficulties non-state actors present in modern conflict situations.

Petrosyan's research greatly enhances our comprehension of contemporary warfare by clarifying non-state actors' crucial involvement and influence on wars. The report offers valuable insights for politicians, military strategists, and security professionals by examining these actors' motivations, capabilities, and strategies. Gaining insight into non-state players' operational and tactical behaviours is crucial, as it exposes their capacity to disrupt, create damage, and inflict casualties in conflicts, even if they do not directly impact the strategic elements. This knowledge provides stakeholders with the essential resources to adjust to the changing characteristics of warfare and formulate efficient tactics to counter the risks presented by non-state actors. Policymakers can use these findings to guide diplomatic efforts, military strategists to customise their approaches to countering insurgencies, and security (including cybersecurity) professionals to strengthen their defence systems.

To advance Petrosyan's research and collaborative efforts, it is crucial to explore further the motivations, tactics, and consequences of non-state actors' participation in conflict. By being thoroughly aware of these elements, politicians, military strategists, and security experts can design strong tactics to effectively fight the risks posed by non-state actors in modern conflict scenarios. Petrosyan's work is an important basis for current conversations and efforts to improve our understanding of the changing nature of conflict and to ensure proactive responses to emerging security concerns worldwide.

3.11. Analysis of International Cybersecurity Governance

Sukumar, Broeders [2] offer a comprehensive analysis of the complex dynamics of the global cybersecurity governance system, focusing mainly on the widespread and significant role of informal methods. The authors analyse the connections between geopolitics, non-state actors, and diplomatic processes to understand how these elements shape the informal institutions that govern cybersecurity. This detailed analysis highlights the crucial importance of informal governance mechanisms, primarily when no official international cybersecurity treaty exists. The authors explain how informal processes facilitate communication and decision making between nation states and non-state players at the United Nations and other international forums.

Their study illustrates how different actors, driven by diverse interests, contribute to the complexity of the regulatory landscape. The military, for instance, emphasises the preservation of cyber capabilities, which may conflict with efforts to maintain stability. Corporations, on the other hand, often prioritise economic gain over security concerns. Intelligence agencies seek to gather information through cyber operations, potentially impacting trust and collaboration. Additionally, national cybersecurity strategies are influenced by both geopolitical and economic considerations.

Raymond and Sherman [63] explained the term "authoritarian multilateralism", which refers to the strategy employed by certain countries, such as China and Russia, to manipulate the processes of multilateral organisations to promote their interests, going against the principles of liberal multilateralism. This deviation from transparency, inclusivity, and accountability highlights a notable change in the worldwide cybersecurity environment, where authoritarian entities exert considerable control over norms and rules. This phenomenon highlights the importance of a detailed grasp on how geopolitics and global cybersecurity governance interact.

Sukumar, Broeders [2]'s research highlights the crucial significance of informal governance in cybersecurity, shifting the usual focus from formal institutions. They support a more thorough investigation of the interactions between states, non-state actors, and informal diplomatic channels, acknowledging the complex nature of the digital environment.

To enhance global cybersecurity, it is necessary for future studies to thoroughly investigate the changing dynamics of informal governance and how it influences policy frameworks. Gaining a comprehensive understanding of these complexities can offer significant perspectives to improve the ability to withstand cyber threats and protect digital systems in our progressively interconnected global environment. By analysing how authoritarian governments shape cybersecurity discussions, scholars can devise tactics to oppose their influence and advocate for a more open, comprehensive, and responsible approach to global cybersecurity governance.

Sukumar, Broeders [2]'s research provides a perceptive analysis of the prevalent informality that defines the worldwide cybersecurity regime. The authors emphasise the significance of understanding the nuances of informal governance institutions by closely examining the relationships between states, non-state actors, and diplomatic procedures. To navigate the complex and evolving digital landscape, a comprehensive understanding of cybersecurity policy and practice is necessary for policymakers and practitioners.

4. Case Studies

Following are three example case studies demonstrating non-state actors' contributions to cybersecurity resilience.

4.1. Case Study 1: Multi-Stakeholder Collaboration in Creating Cybersecurity Standards

The Internet Engineering Task Force (IETF) is a prominent example of non-state actors collaborating to develop cybersecurity standards, including industry experts and academics. The IETF has played a crucial role in formulating technical standards and protocols for the Internet, contributing to establishing cybersecurity norms and best practices. Through open collaboration and consensus-based decision making, the IETF has influenced governance by setting widely adopted standards that enhance cybersecurity resilience on a global scale [64,65].

4.2. Case Study 2: Civil Society Organisations' Role in Cyber Policy Development

The Electronic Frontier Foundation (EFF), a non-profit organisation, has actively participated in shaping cybersecurity governance by influencing policy development and advocating for user privacy and digital rights. Through legal advocacy, public awareness campaigns, and engagement with policymakers, the EFF has influenced the formulation of cybersecurity regulations and guidelines. Their efforts have contributed to establishing norms that prioritise individual privacy and data protection, demonstrating how non-state actors can shape cybersecurity governance through public advocacy and engagement [66,67].

4.3. Case Study 3: Industry-Led Collaborative Initiatives for Cyber Resilience

The Cyber Threat Alliance (CTA), a coalition of cybersecurity companies, exemplifies successful non-state actor contributions to cybersecurity resilience. The CTA has significantly influenced cybersecurity norms and governance by sharing threat intelligence, collaborating on research, and developing best practices. Their collaborative efforts have established industry-wide standards for threat information sharing and collective defence, showcasing how non-state actors within the private sector can proactively shape cybersecurity governance and resilience strategies [68–70].

These case studies demonstrate the tangible impact of non-state actors in shaping cybersecurity norms and governance, highlighting their pivotal role in enhancing cyber resilience through collaborative initiatives, policy advocacy, and technical standardisation.

5. Discussion

This study explored changes in managing cybersecurity, focusing on how non-state actors shape global safety. It conducted a thorough analysis of the present status of cybersecurity and emphasised the changing role of non-state actors in this field. This research provides useful insights into resolving non-state actors' complex challenges in cybersecurity. It highlighted the increasing risks of cyber threats such as supply chain attacks, advanced persistent threats, ransomware, and vulnerabilities on the Internet of Things. It dived into how entities like terrorist organisations exploit cyberspace to pursue their objectives, challenging conventional security methods. Additionally, this study examined how informal processes influence the development of cybersecurity standards. Underlining the significance of fostering collaboration between governmental and non-governmental entities to establish robust security measures, emphasising the role of cyber diplomacy in engaging stakeholders to enhance cybersecurity initiatives.

Our research findings underscored the importance of implementing novel strategies to counter evolving cyber threats while recognising the impact of organisations on diplomatic relations. It emphasised how cooperative approaches complement traditional governance frameworks for effectively addressing cyber challenges. Moreover, this study scrutinised how countries and international organisations approach cyber threats comprehensively. Focusing on the geopolitical implications of managing such challenges, including disparities in technology governance and cooperation, stresses the significance of recognising the geopolitical dimensions of cybersecurity governance to inform the development of policies and strategies tailored to specific geopolitical environments. Furthermore, the analysis emphasised the value of public–private partnerships in enhancing infrastructure resilience against cyber threats. By facilitating information sharing, resource allocation, and response coordination, these partnerships leverage expertise and resources from both the public and private domains, promoting a shared sense of accountability among stakeholders to tackle cyber challenges.

The difficulties in coordination that non-state entities face are a significant aspect that was emphasised. The obstacles encompass various interests, differing levels of competence, and conflicting aims. To overcome these obstacles, enhancing communication, fostering transparent collaboration, and building mutual trust among all parties involved is necessary. This research highlights the significance of policymakers in establishing multi-stakeholder forums and partnerships by emphasising the necessity for improved collaboration. Moreover, offering monetary and regulatory rewards can motivate collaboration between state and non-state actors, promoting a more harmonious cybersecurity ecosystem.

Furthermore, this study highlights the essential need for capacity-building programmes to improve cybersecurity knowledge and resilience. Training programmes, seminars, and information exchange activities are recognised as valuable methods to enhance the capacity of both state and non-state actors to counter cyber threats. By allocating resources to enhance their capabilities, stakeholders can better equip themselves to tackle the ever-changing cybersecurity threats.

5.1. Study Limitations and Future Works

The critique and ideas presented offer significant insights into prospective areas for additional investigation and enhancement within the research on cybersecurity and the involvement of non-state actors. A comprehensive examination of non-state actors' techniques and optimal methods to overcome coordination issues and improve cybersecurity efforts requires thorough investigation. This research could offer practical insights for stakeholders aiming to enhance collaboration in the cybersecurity area by including case studies or empirical evidence, which would provide tangible examples of effective ways. This would facilitate the connection between theoretical concepts and practical implementation, allowing stakeholders to convert abstract frameworks into practical plans.

Also, a more in-depth analysis of the socio-political and economic elements that contribute to the development of cyber threats would enhance the research by offering

a more elaborate comprehension of the fundamental forces that shape the cybersecurity environment. By analysing the broader framework in which cyber threats arise, policymakers and stakeholders can devise more focused and efficient measures to tackle emerging concerns. This comprehensive strategy can aid in reducing risks and developing resilience in a progressively interconnected and intricate digital setting.

Additionally, it is crucial to investigate possible frictions and disputes between state and non-state actors in cybersecurity to foster increased cooperation and confidence. By openly recognising and actively confronting these obstacles, the individuals and groups involved can strive towards constructing more comprehensive and collaborative cybersecurity frameworks. It is necessary to have a sophisticated comprehension of the varied interests and motivations that influence different individuals and take proactive steps to reduce confrontations and encourage productive discussions.

Furthermore, examining the involvement of international organisations and multilateral frameworks in promoting global collaboration in cybersecurity is crucial since this is essential for navigating the intricate geopolitical environment. By analysing the efficiency of current procedures and identifying areas that require enhancement, the research can provide valuable insights to enhance international collaboration and coordination in addressing cybersecurity matters. This involves investigating ways to improve the exchange of information, develop skills, and align policies on a global scale.

It is crucial to offer specific suggestions to policymakers and stakeholders on how to put forward recommended solutions and evaluate their efficacy. This is necessary for turning research findings into tangible results. This research provides practical assistance on policy formulation, implementation methodologies, and performance measurements, enabling stakeholders to enhance cyber resilience proactively. This necessitates a practical strategy that harmonises academic understandings with practical issues, guaranteeing that suggestions are achievable and influential.

Future studies should investigate the changing dynamics of informal governance. Examining how these forces shape and impact cybersecurity governance worldwide will be essential in formulating efficient policies and frameworks to tackle rising cyber threats. By further investigating the complexities of informal governance, researchers can provide valuable insights that inform and direct efforts to enhance cybersecurity resilience and protect digital infrastructures in a progressively interconnected global environment.

5.2. Recommendations for Stakeholders

The changing dynamics of cybersecurity and the growing risks posed by threats underscore the need for a united and forward-thinking approach from both government bodies and companies. The following high-level recommendations are put forth to address cyber threats that relate to geopolitics:

Increased Cooperation and Collaboration: A critical step is enhancing the collaboration between government and non-governmental entities to establish robust and adaptable measures. This collaboration should include engaging in diplomacy and implementing innovative strategies to tackle emerging threats. Measures could involve creating channels for sharing information and coordinating responses.

Engaging with Non-State Actors: Governments should acknowledge the influence of actors such as international non-governmental organisations, businesses, and civil society groups in cybersecurity governance. Collaborating with these actors and utilising their skills and resources can significantly enhance cybersecurity efforts.

Adaptation to Geopolitical Contexts: Understanding geopolitical environments that encompass political, social, and economic aspects is essential for shaping effective cybersecurity frameworks. Governments and businesses should customise their strategies and regulations to protect their digital realms based on the geopolitical factors at play.

Flexibility in Governance Methods: Embracing informal partnerships and adaptable governance methods is crucial to complement traditional structures in cybersecurity gover-

nance. This flexibility allows for prompt responses to changes in threats and weaknesses, making it easier to navigate the complexities of geopolitics.

Enhancing International Cooperation: Considering the varied legal, regulatory, and organisational frameworks governing cybersecurity internationally, fostering cooperation is vital. Governments and businesses must strive towards aligning regulations and exchanging best practices to enhance global digital resilience collectively.

Putting these recommendations into action necessitates a collective effort from government entities, companies, and non-state actors to mitigate the intricate cyber threats and vulnerabilities in the digital warfare era. Policymakers, security professionals, and researchers need to come together to examine the nuanced interplay between geopolitics, governance arrangements/systems, and the rise in cyber threats, setting the stage for a more robust digital landscape. Based on this study, we also recommend the following high-level actions.

In-depth Study of Non-State Actors: An extensive examination of non-state actors is necessary because of their substantial influence on cybersecurity dynamics. Delving deeply into their objectives, capabilities, and strategies can yield critical insights. One approach is to examine case studies of influential non-state actors and their partnerships with state actors in cyber operations.

Investigation of Emerging Threats: Considering the rapidly changing cybersecurity environment, it is imperative to remain informed about emerging threats and vulnerabilities. Subsequent investigations should prioritise the identification and analysis of novel cyber hazards, including those that aim at exploiting nascent technologies such as artificial intelligence, blockchain, and quantum computing.

Assessment of International Cooperation Efforts: It is crucial to evaluate the efficacy of international collaboration mechanisms in tackling cybersecurity threats. This task may entail assessing current frameworks, such as global treaties, accords, and platforms for exchanging information, to determine their strengths, flaws, and areas for enhancement.

Integration of Geopolitical Analysis: Including geopolitical analysis in the study would enhance comprehension of how geopolitical considerations impact state responses and international collaboration in cybersecurity. One such approach is to analyse the geopolitical incentives driving cyber operations, the influence of regional dynamics, and the consequences of power transfers on cybersecurity measures.

Practical Recommendations

Based on this study's analyses, the following are some practical recommendations that policymakers and cybersecurity experts can make to implement cybersecurity strategies and cooperation models.

Case Studies on Successful Public–Private Partnerships (PPPs): Include detailed case studies or practical evidence of successful PPPs in cybersecurity, highlighting the specific policies, frameworks, and collaborative mechanisms that facilitated positive outcomes. For instance, a case study could analyse a successful cybersecurity PPP in a specific industry or region, outlining the policies and regulations that enabled effective collaboration.

Establish Multi-Stakeholder Forums: Policymakers should prioritise the establishment of multi-stakeholder forums that bring together the government, industry, academia, and civil society to foster transparent collaboration and information sharing on cyber threats and highlight specific steps for initiating and maintaining these forums, such as forming committees, setting agendas, and facilitating regular interactions. They can also create work groups in, for instance, ransomware threats and include the public and private sectors to discuss various challenges, needs, etc.

Capacity-Building Programmes: Provide detailed guidelines for designing and implementing capacity-building programmes, including training workshops, seminars, and information exchange activities. These programmes should feed to both state and non-state actors and focus on enhancing cybersecurity knowledge and resilience. Suggestions for

resource allocation, curriculum development, and evaluation metrics for these programmes should be included. Many awareness and training activities can happen online.

Incentivise Collaboration: Offer specific recommendations for policymakers on providing monetary, regulatory, etc., incentives to motivate collaboration between state and non-state actors in cybersecurity. This could involve creating funding schemes, tax incentives, or awards for collaborative initiatives that enhance cybersecurity resilience.

Thorough Investigation of Non-State Actor Techniques: Conduct detailed research on the techniques and optimal methods non-state actors use to overcome coordination issues and improve cybersecurity efforts. Based on the findings, provide actionable insights and practical guidelines to help stakeholders better understand and address these challenges.

Analysis of Socio-Political and Economic Elements: Conduct a comprehensive analysis of the socio-political and economic elements contributing to the development of cyber threats. Offer specific methodologies for policymakers and stakeholders to incorporate this analysis into their cybersecurity strategies, such as integrating economic indicators into risk assessments or conducting political impact analyses on cyber threats.

Recognise and Confront Frictions Between State and Non-State Actors: Guide openly recognising and actively confronting obstacles and disputes between state and non-state actors in cybersecurity. Offer tools and strategies for conflict resolution, promoting productive discussions, and building trust to foster collaborative cybersecurity frameworks.

Enhance International Collaboration through Analysis and Recommendations: Investigate the involvement of international organisations and multilateral frameworks in promoting global collaboration in cybersecurity. Provide specific analysis of the current procedures and identify areas that require enhancement, along with practical recommendations for improving the exchange of information, skill development, and policy alignment on a global scale.

Practical Assistance on Policy Formulation and Implementation: Provide practical assistance to policymakers in formulating, implementing, and evaluating cybersecurity policies. This includes clear steps to propose recommended solutions, evaluate their efficacy, and measure performance (e.g., by creating KPIs), ensuring that all the recommendations translate into tangible results and proactive cyber resilience enhancements.

6. Conclusions

This study used various analyses and provided insights into the complex relationship between cyberspace and the current state of world political cooperation initiatives and the involvement of non-state actors. The review's findings underline the increasing importance of non-state actors, including cybercriminal groups and commercial cybersecurity corporations, in influencing cybersecurity dynamics alongside state actors. Partnerships between government and non-government entities have become more common. This partnership impacts how governments address cyber threats and define international cooperation efforts. It has also emphasised the significance of efficient international collaboration methods in tackling cybersecurity concerns. Public–private partnerships, information-sharing platforms, and international treaties are essential for promoting collaboration and coordination among stakeholders in the global cybersecurity community. The method and findings of this study can be used to investigate the effects of state responses and national and international cooperation on other digital areas.

In the future, it is crucial for research on this subject to prioritise comprehensive investigations of non-state actors. Future studies should examine emerging risks, evaluate international cooperation efforts, incorporate geopolitical analysis, develop policy suggestions, and have the active involvement of stakeholders. By prioritising these areas, the study can help advance the knowledge and understanding of cybersecurity, provide information for policy decisions, and improve global cybersecurity resilience in the era of digital warfare. For instance, the emerging risk of supply chain attacks (which can greatly impact the public and private sectors) and the collaboration between the state and non-state

actors in making proper policy and defining mitigation actions to tackle those attacks should be studied more. The findings of this investigation have significant consequences for politicians, government agencies, cybersecurity professionals, and other individuals responsible for protecting cyberspace. Through a collective and pre-emptive approach, we can tackle the difficulties presented by cybersecurity threats and establish a fortified and robust digital ecosystem that benefits everyone.

Funding: The APC was funded by Anglia Ruskin University.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Johnstone, I.; Sukumar, A.; Trachtman, J. The way ahead for multistakeholder cyber diplomacy. In *Building an International Cybersecurity Regime*; Edward Elgar Publishing: Cheltenham, UK, 2023; pp. 257–265.
2. Sukumar, A.; Broeders, D.; Kello, M. The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemp. Secur. Policy* **2024**, *45*, 7–44. [CrossRef]
3. Liu, J. Rethinking Chinese multistakeholder governance of cybersecurity. In *Building an International Cybersecurity Regime*; Edward Elgar Publishing: Cheltenham, UK, 2023; pp. 185–200.
4. Cîrnu, C.-E.; Rotuna, C.; Vasiloiu, I.-C. Comparative Analysis on Cyber Diplomacy in EU and US. *Rom. Cyber Secur. J.* **2023**, *5*, 77–86. [CrossRef]
5. Sukumar, A. The geopolitics of multistakeholder cyber diplomacy: A comparative analysis. In *Building an International Cybersecurity Regime*; Edward Elgar Publishing: Cheltenham, UK, 2023; pp. 20–58.
6. Ampratwum, G.; Osei-Kyei, R.; Tam, V.W.Y. Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events: A systematic review. *Int. J. Crit. Infrastruct. Prot.* **2022**, *39*, 100556. [CrossRef]
7. Whyte, C.; Mazanec, B. *Understanding Cyber-Warfare: Politics, Policy and Strategy*; Routledge: Abingdon, UK, 2023.
8. Vaismoradi, M.; Jones, J.; Turunen, H.; Snelgrove, S. Theme development in qualitative content analysis and thematic analysis. *J. Nurs. Educ. Pr.* **2016**, *6*, 100. [CrossRef]
9. Ness, S.; Khinvasara, T. Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector. *J. Eng. Res. Rep.* **2024**, *26*, 107–117. [CrossRef]
10. Sigholm, J. Non-state actors in cyberspace operations. *J. Mil. Stud.* **2013**, *4*, 1–37. [CrossRef]
11. Work, J. In wolf's clothing: Complications of threat emulation in contemporary cyber intelligence practice. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019.
12. Kumar, I. Emerging threats in cybersecurity: A review article. *Int. J. Appl. Nat. Sci.* **2023**, *1*, 1–8.
13. Mijwil, M.; Unogwu, O.J.; Filali, Y.; Bala, I.; Al-Shahwani, H. Exploring the top five evolving threats in cybersecurity: An in-depth overview. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 57–63. [CrossRef]
14. Asbaş, C.; Tuzlukaya, Ş.E. Cyberwarfare: War Activities in Cyberspace. In *Handbook of Research on War Policies, Strategies, and Cyber Wars*; Özsungur, F., Ed.; IGI Global: Hershey, PA, USA, 2023; pp. 128–145.
15. Egloff, F.J.; Shires, J. The better angels of our digital nature? Offensive cyber capabilities and state violence. *Eur. J. Int. Secur.* **2023**, *8*, 130–149. [CrossRef]
16. Usman, H.; Mir, S.; Rehman, A. Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2(4) of the UN Charter. *Glob. Leg. Stud. Rev.* **2023**, *VIII*, 16–26. [CrossRef]
17. Thomas, J.E. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *Int. J. Bus. Manag.* **2018**, *12*, 1–23. [CrossRef]
18. Alqudhaibi, A.; Albarrak, M.; Aloseel, A.; Jagtap, S.; Salonitis, K. Predicting cybersecurity threats in critical infrastructure for industry 4.0: A proactive approach based on attacker motivations. *Sensors* **2023**, *23*, 4539. [CrossRef] [PubMed]
19. Ferdous, J.; Islam, R.; Mahboubi, A.; Islam, Z. A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms. *IEEE Access* **2023**, *11*, 121118–121141. [CrossRef]
20. Aslan, Ö.; Aktuğ, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **2023**, *12*, 1333. [CrossRef]
21. Riggs, H.; Tufail, S.; Parvez, I.; Tariq, M.; Khan, M.A.; Amir, A.; Vuda, K.V.; Sarwat, A.I. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors* **2023**, *23*, 4060. [CrossRef]
22. Sjøen, M.M.; Mattsson, C. Depoliticising political violence: State-centric and individualised discourses in the Norwegian counterterrorism policy field. *Scand. J. Educ. Res.* **2023**, *67*, 950–963. [CrossRef]
23. Lilli, E.; Painter, C. 9 Soft power and cyber security: The evolution of US cyber diplomacy. In *Soft Power and the Future of US Foreign Policy*; Hendrik, W.O., Ed.; Manchester University Press: Manchester, WA, USA, 2023; pp. 161–179.
24. Liebetrau, T.; Monsees, L. Assembling Publics: Microsoft, Cybersecurity, and Public-Private Relations. *Politics Gov.* **2023**, *11*, 157–167. [CrossRef]
25. Schaefer, D. Spies and scholars in the cyber age: Researching intelligence in Australian policy and regional security. *Aust. J. Int. Aff.* **2024**, *78*, 102–122. [CrossRef]

26. Petrosyan, M. The Role of Non-State Actors in Modern Warfare: The Case of Syria and Nagorno-Karabakh. *J. Balk. Near East. Stud.* **2024**, *26*, 149–163. [CrossRef]
27. Gabrielli, G. Individual Criminal Responsibility of Non-State Actors Operating in Cyberspace for War Crimes Under the ICC Statute. *EU Comp. Law Issues Chall. Ser. (ECLIC)* **2023**, *7*, 286–315.
28. Madnick, B.; Huang, K.; Madnick, S. The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Inf. Secur. J. A Glob. Perspect.* **2024**, *33*, 204–225. [CrossRef]
29. Shukla, V. A Brief Study of International Law in the Age of Cybersecurity. *EPRA Int. J. Multidiscip. Res. (IJMR)* **2023**, *9*, 269–273. [CrossRef]
30. Maschmeyer, L. Subversion, cyber operations, and reverse structural power in world politics. *Eur. J. Int. Relat.* **2023**, *29*, 79–103. [CrossRef]
31. Azubuike, C.F. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. *Nnamdi Azikiwe J. Political Sci.* **2023**, *8*, 101–114.
32. Maulana, Y.I.; Fajar, I. Analysis of cyber diplomacy and its challenges for the digital era community. *IAIC Trans. Sustain. Digit. Innov. (ITSDI)* **2023**, *4*, 169–177. [CrossRef]
33. Kosenkov, A. Cyber conflicts as a new global threat. *Future Internet* **2016**, *8*, 45. [CrossRef]
34. Abdullahi, A.; Musa, I.G. The legitimacy of international law: Challenges and the emerging issues. *J. Glob. Soc. Sci.* **2023**, *4*, 14–34. [CrossRef]
35. Utkirovich, R.U. Navigating the Cyber Legal Landscape: Protecting Legal Entities through Comprehensive Cyber-security Strategies. *Uzb. J. Law Digit. Policy* **2023**, *1*. [CrossRef]
36. Lewis, E.J.; Baez, M.D. A Critical Analytical View of Control Theory and the Geopolitical and Economic Drivers Affecting Cyber Security Warfare. In *Applied Research Approaches to Technology, Healthcare, and Business*; Burrell, D.N., Ed.; IGI Global: Hershey, PA, USA, 2023; pp. 28–45.
37. Diro, A.; Kaisar, S.; Vasilakos, A.V.; Anwar, A.; Nasirian, A.; Olani, G. Anomaly detection for space information networks: A survey of challenges, techniques, and future directions. *Comput. Secur.* **2024**, *139*, 103705. [CrossRef]
38. Painter, C. US multistakeholder engagement in cyber stability issues. In *Building an International Cybersecurity Regime*; Edward Elgar Publishing: Cheltenham, UK, 2023; pp. 143–164.
39. Zhao, B. Granting legitimacy from non-state actor deliberation: An example of women's groups at the United Nations Framework Convention on Climate Change. *Environ. Policy Gov.* **2023**, *34*, 236–255. [CrossRef]
40. Dunn Cavelty, M.; Smeets, M. Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *J. Eur. Public Policy* **2023**, *30*, 1330–1352. [CrossRef]
41. Sivan-Sevilla, I. Supranational security states for national security problems: Governing by rules & capacities in tech-driven security spaces. *J. Eur. Public Policy* **2023**, *30*, 1353–1378.
42. Radanliev, P. Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *J. Cyber Secur. Technol.* **2024**, 1–51. [CrossRef]
43. Sullivan, J.; Nurse, J.R. *Cyber Security Incentives and the Role of Cyber Insurance*; RUSI Emerging Insights Paper; Technical report; Royal United Services Institute for Defence and Security Studies (RUSI): London, UK, 2021.
44. Heath, B. Before the Breach: The Role of Cyber Insurance Incentivizing Data Security. *Georg. Wash. Law Rev.* **2018**, *86*, 1115.
45. Wolff, J. The role of insurers in shaping international cyber-security norms about cyber-war. *Contemp. Secur. Policy* **2024**, *45*, 141–170. [CrossRef]
46. Arslan, A.S. Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. *APSA Prepr.* 2024; *preprint*. [CrossRef]
47. Iacono, M.; Mastroianni, M. Evaluation of the Effectiveness of National Promotion Strategies for the Improvement of Privacy and Security. *Computers* **2024**, *13*, 87. [CrossRef]
48. Girdhar, K.; Singh, C.; Kumar, Y. AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda. In *Blockchain for Cybersecurity in Cyber-Physical Systems*; Maleh, Y., Alazab, M., Romdhani, I., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 185–213.
49. Tyagi, A.K. Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications. In *AI and Blockchain Applications in Industrial Robotics*; IGI Global: Hershey, PA, USA, 2024; pp. 171–199.
50. Lone, A.N.; Mustajab, S.; Alam, M. A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Secur. Priv.* **2023**, *6*, e318. [CrossRef]
51. Kaur, I.; Gupta, V.; Verma, V.; Kaur, S. Securing healthcare records using blockchain: Applications and challenges. In *AI and Blockchain in Healthcare*; Springer: Singapore, 2023; pp. 57–66. [CrossRef]
52. Vegesna, V.V. Privacy-Preserving Techniques in AI-Powered Cyber Security: Challenges and Opportunities. *Int. J. Mach. Learn. Sustain. Dev.* **2023**, *5*, 1–8.
53. Rees, J.; Rees, C.J. Cyber-Security and the Changing Landscape of Critical National Infrastructure: State and Non-state Cyber-Attacks on Organisations, Systems and Services. In *Applications for Artificial Intelligence and Digital Forensics in National Security*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 67–89.
54. Vegesna, V.V. Enhancing cyber resilience by integrating AI-Driven threat detection and mitigation strategies. *Trans. Latest Trends Artif. Intell.* **2023**, *4*. Available online: https://ijsdcs.com/index.php/TLAI/article/view/396/140 (accessed on 16 October 2024).

55. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors* **2023**, *23*, 6666. [CrossRef]
56. Safitra, M.F.; Lubis, M.; Fakhrurroja, H. Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability* **2023**, *15*, 13369. [CrossRef]
57. Alrumaih, T.N.I.; Alenazi, M.J.F.; AlSowaygh, N.A.; Humayed, A.A.; Alablani, I.A. Cyber resilience in industrial networks: A state of the art, challenges, and future directions. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 101781. [CrossRef]
58. Melaku, H.M. A dynamic and adaptive cybersecurity governance framework. *J. Cybersecur. Priv.* **2023**, *3*, 327–350. [CrossRef]
59. Oppenheimer, H. How the process of discovering cyberattacks biases our understanding of cybersecurity. *J. Peace Res.* **2024**, *61*, 28–43. [CrossRef]
60. Shah, V. Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Rev. Esp. Doc. Cient.* **2021**, *15*, 42–66.
61. Trachtman, J. Developing multistakeholder structures for cybersecurity norms: Learning from experience. In *Building an International Cybersecurity Regime*; Edward Elgar Publishing: Cheltenham, UK, 2023; pp. 85–110.
62. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Inf. Fusion* **2023**, *97*, 101804. [CrossRef]
63. Raymond, M.; Sherman, J. Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice. *Contemp. Secur. Policy* **2024**, *45*, 110–140. [CrossRef]
64. Traitware. Should Governments Require Stronger Security? *2024.* Available online: https://traitware.com/should-governments-step-in-to-require-stronger-cybersecurity-for-companies/ (accessed on 14 October 2024).
65. Nanni, R. Digital sovereignty and Internet standards: Normative implications of public-private relations among Chinese stakeholders in the Internet Engineering Task Force. In *The Geopolitics of Chinese Internets*; Routledge: Abingdon, UK, 2024; pp. 8–28.
66. Anagnostakis, D. The External Face of the EU's Cybersecurity Policies: Promoting Good Cybersecurity Governance Abroad? In *EU Good Governance Promotion in the Age of Democratic Decline*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 237–257.
67. Nhan, J.; Carroll, B.A. The offline defense of the Internet: An examination of the electronic frontier foundation. *SMU Sci. Technol. Law Rev.* **2011**, *15*, 389.
68. Hewling, M. *Cyber Intelligence: A Framework for the Sharing of Data*; Academic Conferences International Limited: Reading, PA, USA, 2018; pp. 637–644.
69. Yatagan, C. *Interaction Between the U.S. Intelligence Community and the Private Sector in Sharing Cyber Threat Intelligence*; American University: Washington, DC, USA, 2022; p. 103.
70. Haklai, B. Cybersecurity Private-Public Partnerships: A Bridge to Advance Global Cybersecurity. *Tex. Tech. Law Rev.* **2023**, *56*, 627–688.