The Rise of State-Sponsored Cyber-attacks: The Case for International Cooperation in Strengthening Defence Systems

By

C.A. Mumma-Martinon, Lucy W. Maina and James J. Kimuyu

Abstract

The recent years have seen an increase in state sponsored acts of cyber-attacks that are becoming increasingly sophisticated. These attacks mainly target nation's critical infrastructure such as communication systems, electricity generation and distribution systems, transportation systems, health support systems and financial services whose collapse and unavailability can lead to partial or total collapse with huge reputation, economic, security and political implications. As organizations and nations grapple with the challenges posed by increasingly sophisticated cyber threats, it is imperative to examine how current cybersecurity strategies are responding to them and if these responses are adequate. Failure to address these challenges portends exposing critical infrastructure, sensitive data, and national security interests to unprecedented levels of danger and disruption. This study therefore seeks to analyze the rise of state-sponsored cyber-attacks and its significance lies in assessing how nations can enhance these capabilities; foster international cooperation and collaboration and strengthen cyber resilience and incident response preparedness. The study has adopted a mixed-methods research design to triangulate data from various documented sources and provide a comprehensive understanding of state-sponsored cyber threatsand cybersecurity strategies. It also provides recommendations such as robust governance structures, increasing investments, strengthening partnerships with allies and international organizations, information sharing and analysis centres, integrate robust incident response, development and training programmes, continuous monitoring and evaluation and eventually further research to be done.

Keywords: *cyber-attacks, state-sponsored, defence systems, international relations, national security.*

Introduction

In recent years, there has been significant increase in the frequency and sophistication of state-sponsored cyberattacks targeting nations' critical infrastructure and sensitive government systems.

There was a 63% increase in state-sponsored cyberattacks globally in the past year alone. These attacks have ranged from espionage efforts aimed at stealing classified information to disruptive operations targeting essential services such as energy, healthcare and finance. (Crowdstrike, 2024). Despite heightened awareness and investment in counter cybersecurity measures, nations worldwide are grappling with substantial challenges in effectively mitigating the threats posed by state-sponsored cyberattacks. According to Verizon, 85% of data breaches involved human elements, (Verizon, 2023). This statistic underscores the increasingly sophisticated social engineering tactics employed by state actors, who leverage psychological manipulation and deception to exploit individuals within target organizations.

Moreover, the global shift towards remote work induced by the Coronairus-19 (COVID-19) pandemic has further exacerbated cybersecurity vulnerabilities on a massive scale. With remote work becoming the new norm, organizations have had to rapidly deploy technologies and infrastructure to support remote operations, often without adequate security measures in place. This hasty transition created fertile ground for cybercriminals, with the coming in of the new norm, there was a staggering 600% increase in phishing attacks targeting remote workers (Anti-Phishing Working Group, 2020).

This study therefore seeks to analyze the rise of state-sponsored cyber-attacks and its significance lies in assessing how nations can enhance these capabilities; foster international cooperation and collaboration and strengthen cyber resilience and incident response preparedness.

Theoretical framework

The theoretical underpinnings that guide the analysis of cybersecurity and cyber warfare and the role of states as perpetrators heavily borrows from both the Realist and Deterrence Theories. From a realist perspective rooted in international relations theory, cybersecurity and cyber warfare may be seen through the lens of power politics and state-centric behaviour, (Waltz, 1979). Accordingly, states are rational actors driven by the pursuit of power and security in an anarchic international system, (Mearsheimer, 2014). In the context of cybersecurity, this perspective informs on the role of states as primary actors in perpetrating cyberattacks and defending themselves against cyber threats and attacks to safeguard their national interests, (Libicki, 2014). Interpreted, empirical evidence supports this perspective as state-sponsored cyber espionage campaigns targeting rival nations and government networks are aimed at retaining sovereignty and gaining advantage and

power. Moreover, the proliferation of offensive cyber capabilities by states, such as the development of cyber weapons and the establishment of military cyber commands, underscores the realist notion of states prioritizing their strategic advantage in cyberspace over each other, (Arquilla & David, 1993).

The Deterrence theory adapted and applied by Libicki, (2009) provides further insights complementing the realist view. From this perspective, deterrence seeks to weaken the effects of cyberattacks to a minimal level at an acceptable cost. The state seeks to deter adversaries from engaging in malicious cyber activities through the credible threat of retaliation or punishment (Schelling, 1980). Studies have explored the effectiveness of deterrence strategies in the cyber domain, examining case studies of state responses to cyberattacks and their impact on adversarie" behaviour. States intentionally mount a cyber-attack for the sole purpose of displaying their capabilities to reduce the likelihood of being under attack (National Research Council, 2010).

Additionally, empirical data on state-sponsored cyber operations and responses, such as the attribution of cyberattacks and public condemnation by victim states, provide insights into the dynamics of cyber deterrence in practice (Nye, 2011). The two theories thus provide ground for analysing motivations by state to cyber-attack as well as the use of attacks to express their state power and safeguard their space. They also assist to analyse how states seek to influence the behaviour of adversaries through deterrence as contrasted with denial strategies that seek to improve technologies and processes to ensure low levels of success by attackers.

Methodology

This study has used a mixed-methods research design to triangulate data from various documented sources and provide a comprehensive understanding of state-sponsored cyber threatsand cybersecurity strategies, (Creswell & Creswell, 2017). Multiple data bases and information sources were used from which data was extracted and analysed qualitatively and quantitatively. Additionally, some data were re-analysed to explore state behaviour in cyberspace, the role of power dynamics in shaping cybersecurity policies and the effectiveness of strategies that are in place to counter cyber threats. The research design allowed mining and analyzing empirical data on cyber incidents, such as data breaches and cyberattacks attributed to state actors, to identify trends and patterns that align with the theoretical frameworks provided.

Data sources for the study included official government documents, academic literature, cybersecurity reports, and empirical datasets on cyber incidents. These were accessed from reputable sources such as government agencies, cybersecurity firms, tech company records and academic institutions. The data were then coded and categorized to extract insights into the topic including the motivations behind state-sponsored cyberattacks and the efficacy of cybersecurity deterrence strategies. By triangulating qualitative and quantitative data through thematic analysis and statistical analysis, this study provided a nuanced understanding of state-sponsored cyber threats, (Bhandari, 2023).

Empirical Literature

This section analyses from empirical literature in terms of: forms of cyber-attacks; evolution and trends in cyber threats; state-sponsored cyberattacks: nature and characteristics; impact on national security and critical infrastructure; current cybersecurity enhancing strategies and frameworks and challenges and shortcomings in countering cyber-attacks.

Forms of cyber-attacks

There are various Tactics, Techniques and Procedures (TTPs) employed by malicious actors in the cyberspace that have been adopted by states who engage in cyberwarfare. One of the most common forms of attack is known as phishing a**nd involv**es gaining unauthorized access to target networks. According to Verizon, (2020), 22% of data breaches involved phishing attacks, highlighting the effectiveness of this social engineering technique in compromising user credentials and delivering malware payloads. In this type of attack, once the hacker accesses the network, they hibernate for certain period of time, to avoid immediate correlations by security policies and detection. The hackers then conduct internal reconnaissance activities to locate critical servers or applications from which to steal confidential data, then gains access using privileged escalations, brute force methods or other mechanisms and performs data exfiltration to send the stolen data to external servers (Abad, 2005; Aburrous *et al.,* 2008; Bin, Qiaoyan and Xiaoying, 2010).

On the other hand, ransomware attacks have become more popular today. This is due to the fact that hackers can quickly gain financial benefits from the victim organizations by encrypting their data and files needed for normal business activities. The hackers then demand ransom payments in exchange for decryption keys. In most cases, businesses pay the ransom to get the locked data

restored and continue with normal business, (Kapoor *et al.*, 2021; Kaur, Dhir & Singh, 2017; Maurya *et al.*, 2018).

The use of Distributed Denial of Service Attack (DDOS) has also gained prominence in the recent past. This type of attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic (Douligeris & Mitrokotsa, 2004; Tayyab, Belaton & Anbar, 2020; Vishwakarma & Jain, 2020). DDOS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic (Huang *et al*., 2020; Nooribakhsh & Mollamotalebi, 2020). DDOS attack can be likened to an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination, thus denying the rightful users the right to use the systems. In response, most organisations end up pulling down the affected ICT System, effectively enabling the attackers achieve their intended purposes.

Data theft, leakages, illegal access and disgruntled employees continue to pose a significant threat to governments and organisations. Despite the good intention, the manner in which the data and information is obtained breaches internal security and confidentiality requirements. Another method of attack is the Zero-Day Exploits which exploits previously unknown vulnerabilities in software and hardware systems (Khandelwal, 2019). For instance, the Stuxnet worm, attributed to state-sponsored actors, leveraged multiple zero-day exploits to target Iran's nuclear enrichment facilities, demonstrating the sophistication of offensive cyber operations (Zetter, 2011). Water holing is another strategy involving the setting up of a fake website or compromising authentic sites for the purpose of exploiting users.

Evolution and Trends in Cyber Threats

The evolution and magnitude of cyber security attacks have been extensively documented through empirical studies, showcasing a trajectory marked by increasing frequency and sophistication. Studies have documented the evolution of cyber threats over time, illustrating the increasing frequency and sophistication of cyberattacks, (Böhme & Stefan, 2009). There is a steady rise in the number of cyber threats detected each year, with a 56% increase in new malware variants in 2020 compared to the previous year, (Symantec, 2021). This surge underscores the relentless

innovation of cybercriminals, who continually adapt their tactics to bypass traditional security measures. Cybercrime damages would cost the world $6 trillion annually by 2021, demonstrating the escalating financial impact of cyber threats, (Computer Crime Ventures, 2021).

State-Sponsored Cyberattacks: Nature and Characteristics

State sponsored cyberattacks have been identified as the most pervasive and diverse with ramifications being quite serious and long-lasting (Thomas & Buchanan, 2015). Espionage, sabotage and influence operations are the primary objectives of state-sponsored cyberattacks (Cyber Threat Alliance, 2020). Moreover, the "MITRE ATT&CK Framework" provides empirical data on the TTPs commonly employed by state actors, including phishing, malware deployment, and exploitation of software vulnerabilities (The MITRE Corporation, 2020).

Reports indicate that Ukraine has experienced numerous state-sponsored cyberattacks the most notable incident being the 2017 *NotPetya* cyberattack, which targeted Ukrainian infrastructure but spread globally, causing billions of dollars in damages to businesses worldwide. This attack, widely attributed to Russia, disrupted critical services in Ukraine, including banks, airports, and government agencies. Another case is that of Iran whereby in 2010, the Stuxnet worm believed to have been developed by the United States and Israel, targeted Iran's nuclear facilities, causing significant damage to its uranium enrichment program. In retaliation, Iran launched cyberattacks against various targets, including U.S. financial institutions and critical infrastructure. Additionally, South Korea has on several occasions faced state-sponsored cyberattacks from North Korea, aimed at disrupting government operations and undermining national security (Feigenbaum & Nelson, 2021). One notable incident is the 2014 cyberattack on Sony Pictures Entertainment, attributed to North Korea, which resulted in the leak of sensitive corporate data and the cancellation of the release of a controversial film (Feigenbaum & Nelson 2021).

The SolarWinds cyberattack, attributed to Russian state-sponsored actors, involved compromising the software supply chain of SolarWinds, a prominent IT management software provider. According to reports from cybersecurity firms such as Fire Eye and CrowdStrike, the attackers inserted malicious code into SolarWinds' Orion software updates, which were then distributed to thousands of organizations, including government agencies and Fortune 500 companies

(Kaspersky Lab, 2021). This sophisticated supply chain attack resulted in unauthorized access to sensitive data and networks further demonstrating the extent of the threat posed by state-sponsored actors to global cybersecurity.

In Kenya, 2023 was a turning point within the Cybersecurity domain. The country faced a massive DDOS attack on the critical eCitizen platform and other critical infrastructure entities rendering the System inaccessible. The attack attributed to the hacktivist group "*Anonymous Sudan*," originated from various international locations. Its intent and motivations remain unclear, but the incident highlighted the potential for severe economic and security implications for the country and led to loss of revenue due to the ongoing digitization of government services while at the same time affecting delivery of crucial government services, (Mwai & Nkonge, 2023).

Impact on National Security and Critical Infrastructure

The most notable characteristic of cyber-attack is the surprise element that it is associated with. Unlike conventional warfare where the threat is known way before an actual attack, cyber-attacks are asymmetrical and at times executed without warning or prior signs. They therefore present great anxiety and are associated with great magnitude of loss or damage. In this regard evidence on cyber espionage from cybersecurity firms, government agencies, and intelligence reports document the pervasive threat of state-sponsored cyber espionage to national security and intelligence interests. For example, the Chinese state-sponsored hackers that targeted the USA jeopardized intellectual property and trade secrets provides empirical data on the scope and scale of such operations (U.S. Department of Justice, 2020).

Cyber-attacks have the capability to cause massive disruption of critical infrastructure such as energy, transportation, and healthcare systems. They have the potential to disrupt government operations that are delivered through online platforms. The 2021 Cybersecurity Insights Report by the International Business Machines (IBM) highlights the increasing frequency of cyberattacks targeting critical infrastructure, with 59% of surveyed organizations reporting a rise in such incidents. Reports from incident response investigations and forensic analysis of cyber incidents provide insights into the tactics and techniques used by state-sponsored actors to disrupt essential services and undermine national security (IBM Security, 2021).

Current Cybersecurity Enhancing Strategies and Frameworks

Comparing strategies is often complicated venture given the nature of attack is a confounding variable in many of the cases. According to McLean, (2017), traditional perimeter-based defences remain prevalent, they are insufficient in addressing the evolving tactics of cyber adversaries. Perimeter-based defenses fail to detect and mitigate insider threats or advanced persistent threats that bypass perimeter defences through techniques like social engineering or zero-day exploits, (McLean, 2017).

The Cybersecurity Framework was developed by the National Institute of Standards and Technology (NIST) and is widely recognized and adopted framework for improving cybersecurity risk management. The framework provides a flexible and customizable approach to managing cybersecurity risks, offering guidance on identifying, protecting, detecting, responding to and recovering from cyber threats. Organizations can use the NIST Cybersecurity Framework to assess their current cybersecurity practices, identify gaps, and prioritize investments to improve their overall cybersecurity resilience, (NIST, 2024).

Studies have identified several challenges and gaps in cybersecurity defence mechanisms that hinder effective cyber threat mitigation (Dhillon & Sushil, 2015). There is shortage of skilled cybersecurity professionals as a significant challenge faced by organizations worldwide, with 61% of surveyed companies reporting a shortage of cybersecurity expertise, (IBM Security, 2021). Moreover, only 38% of organizations have a formal cybersecurity strategy in place, indicating a gap in strategic planning and implementation, (PwC, 2021). The shortage of skilled professionals hampers organizations' ability to effectively defend against cyber threats, as they may lack the necessary talent to develop and implement robust security measures, monitor systems for potential breaches, and respond to cyber incidents in a timely manner. Without a comprehensive strategy, organizations may struggle to prioritize cybersecurity investments, align security initiatives with business objectives, and effectively coordinate cybersecurity efforts across departments and stakeholders. This lack of strategic planning leaves organizations vulnerable to cyber threats and increases the likelihood of security breaches.

While different nations have adopted varied approaches and strategies for ensuring cyber security, there is an evolving culture of best practices that arise from the works of cyber security firms and tech companies in the USA and Europe. The US for instance has in place the Cybersecurity and Infrastructure Security Agency (CISA) which regularly publishes reports and assessments of national cybersecurity policies and initiatives. The country's cybersecurity strategy and implementation plan provide an overview of the U.S. government's approach to cybersecurity, including priorities, goals, and action plans. Additionally, the National Cyber Strategy outlines strategic objectives and initiatives aimed at enhancing cybersecurity resilience and combating cyber threats. On the other hand, the European Union Agency for Cybersecurity (ENISA) produces empirical data on national cybersecurity policies and initiatives across the EU member states indicating a modicum of international cooperation. The Annual Cyber Security Strategy Reports assess the implementation of national cybersecurity strategies and highlight best practices and areas for improvement. Furthermore, the EU Cybersecurity Strategy outlines policy objectives and legislative initiatives to strengthen cybersecurity cooperation and resilience at the European Union level, (European Commission, 2022).

The African continent action on cyber security has been slow and the continent lags behind in governance, laws and regulations, technical capacity, research and development, training among others. However, countries such as South Africa, Nigeria, Ghana and Kenya have made some strides in putting up Cybersecurity structures and in the development of a Cybersecurity posture for a more secure cyberspace. For instance, Kenya's **Cybersecurity Posture** is exemplified by the National Computer and Cybercrimes Coordination Committee (NC4), the Communications Authority of Kenya (CA) and the National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) who work jointly to coordinate cybersecurity efforts and response to cyber incidents.

Kenya also has in place several policies and frameworks to guide its cybersecurity initiatives including the Computer Misuse and Cybercrimes Act (CMCA), 2018, the Kenya Information and Communications Act (KICA), 1998 and the Data Protection Act of 2019 which provide legal frameworks for cybersecurity and data protection. Additionally, the National Cybersecurity Strategy, 2022 – 2027 and the CMCA, 2018 Regulations, provide a roadmap for improving

cybersecurity resilience and enhancing coordination among stakeholders. The implementation of these strategies is incumbent upon capacity building, public-private collaboration and adequate funding for cybersecurity initiatives to counter the evolving nature of cyber threats.

Challenges and Shortcomings in Countering Cyber-attacks

This section incorporates attribution challenges, sophistication of tactics, skill shortage, under-investment in cyber resilience and implications for national security and international cooperation in strengthening defence systems.

Attribution Challenges

Empirical data from cybersecurity incident response and forensic investigations reveal the difficulties in accurately attributing cyberattacks to state-sponsored actors. According to Fire Eye, (2020), the complexity of attribution due to the use of false flag tactics, proxy servers and encrypted communications by malicious actors. This evidence underscores the challenge of holding state actors accountable for cyber aggression and enforcing consequences. Attackers can deliberately manipulate digital evidence to make it appear as though the cyberattack originated from a different source than the actual perpetrator. This deceptive technique complicates attribution efforts at times leading investigators to attribute the attack to the wrong entity based on false information, highlighting the challenge of accurately identifying state-sponsored actors behind cyberattacks, (Fire Eye, 2020).

Sophistication of Tactics

Analysis of cyber incidents attributed to state-sponsored actors demonstrates the increasing sophistication of their tactics and techniques. The MITRE ATT&CK Framework provides data on the use of Advanced Persistent Threats (APTs) by state actors, including reconnaissance, lateral movement and data exfiltration techniques, (The MITRE Corporation, 2020). This empirical evidence illustrates the evolving nature of cyber threats and the challenge of defending against state-sponsored cyber aggression using traditional cybersecurity approaches.

Skill shortage

Skill shortage is another challenge in countering cyber-attacks. Skilled cybersecurity professionalsis a significant gap in current cybersecurity approaches. ISC2 Cybersecurity Workforce Study,

(2023), found that the global shortage of cybersecurity professionals reached 3.1 million in 2020, representing a 63% increase since 2019. The United States faced a shortage of over 500,000 cybersecurity professionals in 2020. Similarly, the United Kingdom faced a shortage of over 140,000 cybersecurity professionals in the same year. This shortage has been exacerbated by factors such as the increasing demand for cybersecurity expertise across various sectors, the prevalence of cyber threats targeting states and the poaching of professionals to work remotely from across the globe. This shortage is further exacerbated by the rapid growth of cyber threats, the evolving nature of cybersecurity technologies, and the lack of adequate cybersecurity education and training programs (ISC2 Cybersecurity Workforce Study, 2023).

Under-investment in Cyber Resilience

The analysis of cybersecurity budgets and expenditures reveals a gap in investment in cyber resilience measures, such as incident response planning and cyber insurance. Surprisingly, only 35% of organizations have a dedicated cyber resilience budget, with the majority of cybersecurity spending focused on prevention and detection capabilities, (European Commission, 2022). While this challenge is most often felt in developing countries, it also affects big economies. Germanyhas been cited to have gaps in investment in cyber resilience and that a significant cyber security spending is allocated to prevention and detection capabilities and less on response and insurance. Australia has many organizations focusing their cybersecurity spending on prevention and detection capabilities at the expense of other areas. This evidence suggests a need for organizations to prioritize investments in cyber resilience to mitigate the impact of cyber incidents and enhance overall cybersecurity posture, (European Commission, 2022).

Implications for National Security and International Cooperation in Strengthening Defence Systems

Cyber security is inextricably connected to global security and therefore attracts the attention to international relations. The International Telecommunication Union (ITU) highlights the correlation between geopolitical tensions and cyber threat activity, with state-sponsored actors targeting adversaries' critical infrastructure and strategic assets. State-sponsored cyber operations are aimed at advancing geopolitical interests and often target military organizations, government systems, financial and foreign governments. Often, such attacks are used to generate revenue,

gather intelligence, and or exert influence on the international stage. Attacks such as those advanced by Iran and North Korea among others highlight the complex interplay between state's regional and global geopolitical strategies.

Despite the nature and character of cyber security as a global threat, the normative framework underpinning counter measures reflect gaps and ambiguities. One of the most visited section of international law applicable to cyber operations is the Talinn Manual 2.0 seeking to regulate state behaviour on the cyberspace and mitigate the risk of conflict escalation. In implementing cyber security laws, nations have to grapple with definition of what can be considered acceptable behaviour in cyberspace, as informed by analysis of international agreements and norms.

Additionally, and as observed elsewhere in this study, cyberattacks attribution can be challenging due to the complexities of cyber operations and the ability of attackers to obfuscate their identities. In a case such as that of the Stuxnet attack by the US and Israel targeting Iranian nuclear programme, while the attack is associated with specific actors, the challenges of attribution persist due to the covert nature of cyber operations and the use of advanced obfuscation techniques. This particular attack raised the significant question about the applicability of existing international law to cyberspace. The same case was observed regarding the *WannaCry* attack to the North Korean state-sponsored cyber group known as Lazarus Group. This incident in particular highlighted the urgent need for international cooperation and coordination to address cyber threats effectively. Despite widespread condemnation of the attack and calls for collective action to enhance cyber security, efforts to achieve collective cyber security have been minimal. However, achieving consensus on these issues requires ongoing dialogue and collaboration among governments, international organizations and other stakeholders.

Lastly, the characteristics of cyberattacks are such that no nation can claim to have total safeguards against it. Even when safeguards are in place, cyber-attacks take the form of *moving target* and every safeguard is only valid for a short time while prediction of likely threats can never be totally accurate. Analysis of global cybersecurity trends and threat intelligence data reveals the dynamic and evolving nature of the cyber threat landscape. There is increasing frequency and sophistication of cyberattacks, with state-sponsored actors posing significant challenges to national security and critical infrastructure. This underscores the urgency for nations to collaborate and innovate in

enhancing cybersecurity capabilities to address emerging threats effectively, (IBM Security, 2021).

Additionally, cybersecurity incident reports and economic impact assessments highlight the significant financial and reputational costs of cyberattacks for nations and organizations. For example, the 2020 report on Cost of a Data Breach by the IBM and the Ponemon Institute estimates that the average cost of a data breach is $3.86 million, with higher costs associated with state-sponsored cyber incidents. This further underscores the imperative for nations to pool together to strengthen their cybersecurity defences to mitigate the impact of cyber threats and protect national interests. (IBM Security, 2021).

Conclusion

This study has carefully examined case studies of cyber-attack incidents, their typologies and evolving nature and characteristics. It further analyses impacts of cyber-attacks on national security and infrastructure and the strategies that states have adopted to counter them providing a comprehensive critique on why these strategies and frameworks have failed in the face of modifying and increasing sophistication characterising present day attacks. Clearly, there are challenges further undermining cyber security such as attribution dilemma, greater sophisticating that affords more anonymity to aggressors, skill shortages and under-investment in cyber security emerging from the study. The Realist and Deterrence theories provided vital analytical lenses that aided not only the analysis of drivers of cyber-attacks but allowed an examination of gaps in strategies adopted by nations to counter them. Against the backdrop of identified challenges and shortcomings, the paper delved into the strengths of existing cybersecurity capabilities and strategies and the great opportunity for cooperation in counteracting cyber-attacks.

Recommendations

- **Elect Robust Governance Structures**

  Lessons emerging from the study attest that there is a need for states to put in place robust governance structures to manage their national cyberspace. This should go hand in hand with continually developing articulate cyber deterrence policies, laws and regulations to anchor cybersecurity and cyber warfare operations. It is not sufficient for countries to have their own

cyber security domestic laws which calls for the involvement of regional security mechanisms. These policies, laws and regulations should encompass diplomatic, economic, and military responses to cyber threats and attacks. There is evidence that clear cyber deterrence policies, laws and regulations alongside promoting international norms of responsible behaviour in cyberspace could ward-off adversaries. Additionally, efforts to bolster offensive cyber capabilities, including developing advanced cyber weapons and conducting cyber operations to dissuade adversaries from engaging in hostile cyber activities have great potential for success. Enforcing cybersecurity standards is crucial for maintaining trust, attracting investments, and safeguarding national economic interests.

- **Increasing Investments in Cyber Security**

  This is paramount and requires setting aside funding to continually audit and secure sectors such as telecommunications, finance and banking, government systems, energy, transportation, and healthcare which are often targeted. Such funding can incentivize organizations to invest in advanced cybersecurity measures thus strengthening their overall security posture. Additionally, the adoption of cyber insurance policies can help mitigate financial losses and facilitate recovery from cyber incidents. Businesses and organizations require to set aside critical funding to mitigate cyber threats, ultimately strengthening nations overall incident response capabilities.

- **Strengthening Partnerships With Allies and International Organizations**

  This will assist in coordination of deterrence efforts against state-sponsored cyber aggression has great potential and this should include sharing of information with partners, imposing collective consequences on aggressor states and building resilience. This should also go hand in hand with involvement and ratification of international cybersecurity and cybercrimes conventions such as the Budapest convention on cybercrimes by the Council of Europe and the Malabo conversion on Cybersecurity and personal data protection by the African Union (AU). Partnerships with international organizations such as the United Nations Office on Drugs and Crime (UNODC), the AU and the ITU to access empirical data, success case studies, and best practices in cybersecurity are an imperative.

- **Information sharing and analysis centres (ISACs)**

  This will enhance cybersecurity coordination and response capabilities which are imperative. This is tied to collaborative cybersecurity efforts to protect critical infrastructure. Establishing sector-specific ISACs facilitates real-time information sharing and coordinated responses to cyber threats and is tantamount to fostering a more resilient cybersecurity ecosystem. Establishing ISACs enhances the ability to detect and respond to cyber threats promptly, minimizing potential disruptions.

- **Integrate robust incident response**

  Like in other forms of enhancing security, cyber security strategies have to integrate robust incident response plans for effectively mitigating and responding to cyber incidents. By developing and regularly testing incident response plans at the national and sectoral levels, nations can ensure a coordinated and timely response to cyber incidents, minimizing their impact on critical infrastructure, government systems, and the economy.

- **Development and training programmes**

  Further, investing in cybersecurity workforce development and training programmes will go a long way in improving skills and expertise of incident response personnel, enabling them todetect, contain, and remediate cyber threats more effectively. This goes hand in hand withbuilding a resilient cybersecurity ecosystem and enhancing the country's ability to respond to cyber incidents.

  Due to underdevelopment of systems for mitigating cyber security in developing countries, there will be need to strengthen cybersecurity capacity-building efforts in and across these nations. Leaving behind a great majoring of populations will not achieve global cyber security since they may become the havens to launch attacks. Through technical assistance programs, systematic training and knowledge-sharing initiatives, advanced nations can collaborate with the not-so-endowed nations to help improve cybersecurity capabilities in these countries, promoting a more inclusive and resilient global cyber ecosystem. In response, developing countries should express their interest in securing their cyber space by investing in support infrastructure, offensive cyber capabilities and amplifying their deterrence efforts.

Due to the changing nature of cyber security, continuous research towards developing resilient technologies and defence mechanisms should be promoted. This will entail more engagement with private sector and academia. Collaborative efforts between government agencies, private companies, and academic institutions in sharing case studies, conducting joint research projects, and organizing workshops and seminars to disseminate best practices emerging from lessons in cybersecurity resilience should be encouraged. Such engagements will in addition provide valuable insights into global cybersecurity trends, emerging threats, and effective mitigation strategies, for incorporation into cybersecurity policies and practices.

- **Continuous monitoring and evaluation**

  These practices includes regular assessments will help identify gaps, measure progress and refine strategies. This ensures that efforts remain aligned with evolving cyber threats and organizational needs. This will also inform development of multi-layered defence Strategies which emerge from best practices to mitigate cyber risks effectively. From documented evidence, continuous monitoring and threat hunting has great potential to fall stall attacks underscoring the importance of proactive threat detection and response capabilities in enhancing cybersecurity resilience and minimizing the impact of cyber incidents.

- **Recommendations for Future Research**

  Future research may delve into how countries can cooperate to develop advanced threat monitoring, detection, prevention and response techniques that may aid in mitigating such attacks. More research is needed towards attribution capabilities to accurately identify and correctly attribute state-sponsored cyberattacks. Secondly, as stated, there are gaps in policy, law and regulation development efforts. Future research and policy initiatives should leverage empirical evidence and stakeholder input to develop consensus-based norms and mechanisms for enforcing compliance to cyber space regulations.

References

Abad, C. (2005). The economy of phishing: a survey of the operations of the phishing market. First Monday 10, 1–11. doi:10.5210/fm.v10i9.1272.

Aburrous, M., Hossain, M. A., Thabatah, F. and Dahal, K. (2008). Intelligent phishing website and reporting. International Journal of Security and Networks, 12(3), 188.

Anti-Phishing Working Group (2020). Phishing Activity Trend Report. 1st Quarter 2020 Plus COVID-19 Coverage. May 2020. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf?g

Arquilla, J. and David R. (1993). Cyberwar is coming!. Comparative Strategy 12.2 (1993): 141-165.

Bhandari, P. (2023, June 22). *Triangulation in Research | Guide, Types, Examples*. Scribbr. Retrieved May 18, 2024, from https://www.scribbr.com.

Bin, S., Qiaoyan, W. and Xiaoying, L. (2010). A DNS based anti-phishing approach. In second international conference on networks security, wireless communications and trusted computing, Wuhan, China, April 24–25, 2010. (IEEE), 262–265. doi:10.1109/NSWCTC.2010.196.

Böhme, R. and Stefan K. (2009). Models and Measures for Correlation in Cyber-Threat Defense. Proceedings of the 2009 ACM Workshop on Cyber Security (pp. 57-66). ACM, 2009).

Computer Crime Ventures (2021) Annual Cybercrime Report- 2021. Retrieved on 12th January 2024. Available at: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.

Creswell, J. W. and Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed Methods Approaches. Sage publications.

Crowdstrike Global Threat Report, (2024). Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report. Media contact. Timo Burbidge. timo.burbidge@uk.verizon.com.

Cyber Threat Alliance (2020). Cyber Threat Intelligence Estimate.

DBIR (2023). Data Breach Investigations Report 2023. Verizon 2021.

Dhillon, G. and Sushil, S. (2015). Cybersecurity in the Cloud: Risks and Strategies. Information Systems Frontiers 17.2 243-258.

Douligeris, C. and Mitrokotsa, A. (2004). DDOS attacks and defense mechanisms; classification and state-of-the-art. Compt. Netw. 2004, 44, 643–666.

European Commission (2022). European Cybersecurity Investment Platform. European Union.

Feigenbaum, E. Aand Nelson, M. R. (2021). The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way. Carnegie Endowment For International Peace.

Fire Eye (2020). M-Trends 2020 Special Report. https://www.mandiant.com/sites/default/files/2021-09/mtrends-2020.pdf

Huang, K., Yang, L.Y., Yang, X., Xiang, Y., Tang, Y.Y. (2020). A low-cost distributed denial-of-service attack architecture. IEEE Access 2020, 8, 42111–42119.

IBM Security (2021). Cybersecurity Insights Report. IBM, 2021.

ISC2 Cybersecurity Workforce Study (2023). How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. IS2.

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G. and Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: A review and Future Directions. Sustainability, 14(1), 8. https://doi.org/10.3390/su14010008.

Kaspersky Lab. (2021). Solarwinds Cyberattack: What We Know And What We're Doing To Learn More. Retrieved from https://www.kaspersky.com/blog/solarwinds-cyberattack/37932/

Kaur, G., Dhir, R. and Singh, M. (2017). Anatomy of ransomware malware: Detection, analysis.

Khandelwal, S. (2019). A Deep Dive into Zero-Day Vulnerabilities and Exploits. International Journal of Computer Applications, 180(40), 1-6.

Libicki, Martin C. (2009). Cyber-deterrence and Cyberwar. RAND Corporation, 2009.

Libicki, Martin C. (2014). Cyberspace is not a warfighting domain. Strategic Studies Quarterly 8.3 (2014): 34-65.

Maurya, A. K., Kumar, N., Agrawal, A. and Khan, R. A. (2018). Ransomware evolution, target and safety measures. International Journal of Computer Sciences and Engineering, 6(1), 80–85. https://doi.org/10.26438/ijcse/v6i1.8085

McLean, C. (2017). Beyond the perimeter: The need for early detection and response in the strategies of cybersecurity. Journal of Cybersecurity 3.1 (2017): 29-42.

Mearsheimer, J. (2014). The tragedy of great power politics. W.W Norton & Company, 2014.

Mwai, P. and Nkonge, A. (2023). *Kenya Cyber-Attack: Why is eCitizen down?* BBC World Africa. https://www.bbc.com/news/world-africa-66337573.

National Research Council (2010). *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*. National Academies Press.

NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0. Available at https://doi.org/10.6028/NIST.CSWP.29.

Nooribakhsh, M. and Mollamotalebi, M. (2020). A review on statistical approaches for anomaly detection in DDOS attacks. Information Security Journal. A Global Perspective. 29, 118–133.

Nye, Joseph S. (2011). Deterrence And Dissuasion In Cyberspace: Strategic Studies Quarterly 5.4 (2011): 38-55.

PwC (2021). The Global State of Information Security Survey 2021. PwC, 2021.

Schelling, T. (1980). The strategy of conflict. *Harvard University Press.*

Symantec (2021). Internet Security Threat Report 2021. Symantec.

Tayyab, M., Belaton, B.; and Anbar, M. (2020). ICMPv6-based DoS and DDOS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. IEEE Access, 8, 170529–170547.

The MITRE Corporation. (2020). MITRE ATT&CK® Framework. The MITRE Corporation, 2020.

Thomas, R. and Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies 38.1-2 (2015): 4-37.

U.S. Department of Justice. (2020). Indictment of Chinese state-sponsored hackers for cyber espionage activities. Retrieved from [URL] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

Verizon (2020). Data Breach Investigations Report 2020. Verizon

Verizon (2023). Data Breach Investigations Report 2023. Verizon

Vishwakarma, R. and Jain, A.K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication System, 73, 3–25.

Waltz, Kenneth N. (1979). Theory of International Politics. McGraw-Hill Higher Education, 1979.

Zetter, K. (2011). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group.