Article

Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks

Nnamdi Azikiwe Journal of Political Science (NAJOPS).
2023, Vol. 8(3)
ISSN: 2992-5924

AZUBUIKE, Callistus Francis
Department of Political Science,
Nnamdi Azikiwe University,
Awka, Anambra Nigeria.

Abstract
The world's increasing dependence on technology and global connectivity has made it effortless for people worldwide to connect, communicate, conduct business, engage in training, socialize, and even participate in military activities. This connectivity is facilitated by the internet, computers, and internet-enabled devices, driven by advancements in the information and communication sector. However, this digital age of internet of things has brought about a surge in cyber-attacks, leading to a heightened focus on cybersecurity at the global level. This research seeks to understand why states engage in cyber-attacks during international conflicts and assess the impacts on global peace and security. To address these questions, we explore the motivations, consequences, and impact of state-sponsored cyber-attacks. Our analysis reveals that economic and political interests, national security concerns, and technological capabilities are key motivators behind such attacks. The research methodology involved secondary data collection, content and historical analysis, and the application of securitization theory, which interprets security threats as politically constructed issues requiring exceptional measures. In response to emerging global security challenges, the study emphasizes the need for a comprehensive approach to prevent and respond to state-sponsored cyber-attacks, including diplomatic, legal, and technical measures. We recommend the development of international norms and standards for cybersecurity to foster a shared understanding of cyber threats and enhance international cooperation in addressing these evolving threats.

Keywords
Cyber Security, Cyber-Attacks, Securitization Framework, International Conflicts, International Norms.

Introduction

Cyber security, as stated by Kumar and Somani (2018), encompasses two crucial aspects, the vulnerability that arises due to the emergence of this new digital realm and the implementation of measures and protocols to establish a progressively secure environment. The concept entails a wide range of technical and non-technical practices aimed at safeguarding the integrity and confidentiality of both the digital infrastructure and the sensitive information it carries. According to Kumar and Somani (2018), the field of cyber security involves addressing the inherent risks and insecurities that arise in the digital space. This recognition acknowledges the potential threats that can compromise the integrity of systems and data, while on the other hand, cyber-attack refers to deliberate actions taken by individuals, groups, or nation-states to compromise or exploit computer systems, networks, or digital infrastructure with the intention of causing damage, theft, disruption, or unauthorized access to information. Cyber-attacks can take various forms, including malware infections, phishing, distributed denial-of-service (DDoS) attacks, ransomware, or social engineering. The motivations behind cyber-attacks can range from financial gain to espionage, activism, or geopolitical interests. Cybersecurity on the other hand encompasses the measures and practices implemented to protect computer systems, networks, and data from unauthorized

Corresponding Author:
Azubuike, Callistus Francis, Department of Political Science, Nnamdi Azikiwe University, Awka.
Email: cf.azubuike@unizik.edu.ng

access, damage, disruption, or theft. It involves the application of technologies, policies, and practices to prevent, detect, and respond to cyber threats and vulnerabilities. Effective cybersecurity involves a multi-layered approach, including network security, data encryption, access controls, threat intelligence, incident response, and user awareness and education, (Tushar P. Parikh and Ashok R. Patel 2017)

The increasing reliance on technology and connectivity has made cybersecurity a vital issue globally. In recent times, state-sponsored cyberattacks have become a common occurrence, posing significant threats to international relations and security. According to a report by the Center for Strategic and International Studies (CSIS), state-sponsored cyberattacks have increased by 60% over the last six years, with China, Russia, Iran, and North Korea among the top perpetrators (CSIS, 2020). The scale and scope of these attacks suggest that cyber warfare is becoming a key tool in international conflict. Cybersecurity is crucial for protecting critical infrastructure, sensitive information, and government systems from cyber threats. State-sponsored cyberattacks involve one government attempting to penetrate another government's networks and computer systems for various reasons, such as espionage, disruption of critical infrastructure, and interfering with political processes. Cyberattacks can have significant implications for national security, economic stability, and foreign relations. For instance, the 2016 Russian interference in the U.S. presidential election and the recent Solar Winds attack demonstrate the potential impact of state-sponsored cyberattacks on democratic institutions and international relations. (Janczewski & Colarik, 2017, p. 3).

Understanding the motivations behind state-sponsored cyberattacks is essential for developing effective strategies to prevent and respond to them. Some of the motivations behind these attacks include political, economic, and military objectives. For instance, a country may conduct cyber espionage to gain a competitive advantage in trade or to steal sensitive military or government information (Janczewski & Colarik, 2017). Additionally, cyberattacks can be used to influence political processes or sow discord among populations. Understanding these motivations is crucial in developing effective policies and responses to cyber threats and the impact of state-sponsored cyberattacks in the context of international politics and conflict. The study will help policymakers, governments, and cybersecurity professionals to develop effective strategies for preventing and responding to cyber threats. For instance, the European Union has developed a joint communication on resilience, deterrence, and defense, emphasizing the need for a comprehensive approach to cybersecurity that includes diplomacy, legal measures, and technical solutions (Council of the European Union, 2017).

Additionally, this study will contribute to the existing body of knowledge on cybersecurity and international relations. Previous studies have highlighted the role of cyber warfare in international conflict, and this study builds on these insights by analyzing state-sponsored cyberattacks in the context of international conflict. For instance, Cybersecurity and Geopolitics: National Security Imperatives edited by Choucri and Clark (2018) provides a comprehensive overview of cybersecurity challenges and their impact on global security. State-sponsored cyberattacks are becoming an increasingly important tool in international conflict. Understanding the motivations, impact, and prevention of these attacks is essential for maintaining international relations and security. This study seeks to analyze state-sponsored cyberattacks in the context of international conflict and identify best practices for preventing and responding to these attacks.

In order to fully interrogate this research topic, the following research questions were raised to direct our work, thus; what motivates state-sponsored cyber-attacks in the context of international conflicts? This research question aims to delve into the underlying motivations and objectives that drive states to engage in cyber-attacks as tools of conflict. It involves understanding whether these motivations are primarily political, economic, or strategic in nature. What are the impact and consequences of state-sponsored cyber-attacks on international relations and security? This question focuses on assessing the tangible and intangible consequences of state-sponsored cyber-attacks on the affected states' international relations, their security posture, and the broader global security landscape. It may involve examining case studies

to illustrate the various impacts. How can the international community effectively mitigate and respond to state-sponsored cyber-attacks in times of conflict? This research question explores strategies, policies, and international cooperation mechanisms that can be employed to prevent, mitigate, and respond to state-sponsored cyber-attacks during times of international conflict. It addresses the challenges of attribution, deterrence, and norm development in cyberspace. Providing answers to these questions will aid in achieving the objectives of this research work which are to analyze the changing landscape of cyber threats and their impact on international political relations over the past decade, assess the effectiveness of cyber security policies and strategies implemented by various states and international actors in responding to cyber threats and thereby evaluate the role of cyber incidents in shaping diplomatic interactions and cooperation among nations on the global stage during the specified period.

Literature Review

Cybersecurity has become a significant issue in the realm of international relations due to the increasing dependence on technology and cyberspace in various sectors of the economy, including finance, healthcare, and critical infrastructure (Bachmann, 2018). As such, the security of cyberspace has become a critical concern for governments and private entities alike, with cyber threats posing a significant risk to national security and international stability (Gartzke & Lindsay, 2019). The importance of cybersecurity in international relations is further highlighted by the potential impact of cyber-attacks on democratic institutions and international relations, as seen in the 2016 Russian interference in the U.S. presidential election and the recent Solar Winds attack (Janczewski & Colarik, 2017).

Evolution of Cyber Threats and Vulnerabilities

The evolution of cyber threats and vulnerabilities has undeniably had a significant influence on the dynamics of international politics from 2010 to 2023. Scholars and experts in the field have offered various opinions on this matter which we will be exploring here. The evolution of cyber threats have introduced and also caused the escalation of State-Sponsored cyberattacks in the international politics. Some scholars argue that the proliferation of state-sponsored cyberattacks has reshaped international politics by introducing a new dimension of conflict. These attacks, often attributed to nation-states, have targeted critical infrastructure and government systems, resulting in diplomatic tensions and strategic reevaluations.

As Krekel et al. (2021) note, "State-sponsored cyber operations have blurred the lines between traditional warfare and cyber conflict, forcing nations to adapt their strategies and alliances accordingly." The evolution of cyber threats has also been seen as a catalyst for shifting power dynamics among nations. Arquilla (2017) argues that "cyber capabilities have become a great equalizer in international relations," allowing smaller states to exert influence and challenge traditional superpowers. This shift has compelled states to reconsider their geopolitical strategies.

The development of norms and normative frameworks in cyberspace has been a subject of debate. Some scholars, such as Tallinn Manual 2.0 (Schmitt, 2017), emphasize the importance of establishing rules and norms in cyberspace to mitigate the impact of cyber threats on international relations. Others, like Nye (2015), argue that despite efforts to develop norms, significant challenges remain in enforcing them, which affects their impact on international politics. Cyber incidents have often strained diplomatic relations between nations. According to a study by Rid and Buchanan (2019), "Cyber incidents, even those falling short of armed attacks, have had a noticeable impact on diplomatic discourse, leading to accusations, retaliatory actions, and distrust among states." The influence of cyber threats on international politics extends to the realm of cooperation.

Scholars like Deibert and Rohozinski (2010) argue that increased cyber insecurity has hindered international cooperation on global challenges such as climate change and counterterrorism. The need for collaborative cybersecurity efforts has become more pressing. The evolution of cyber threats has not only affected political dynamics but also has economic and technological implications. Ollivant (2016)

suggests that governments' investments in cyber capabilities have altered economic priorities and raised questions about the dual-use nature of cyber technologies. The evolution of cyber threats and vulnerabilities has indeed influenced the dynamics of international politics from 2010 to 2023 in multifaceted ways. It has led to changes in power dynamics, the development of norms, strained diplomatic relations, and implications for international cooperation. These opinions from scholars underscore the complexity of the issue and the need for a nuanced understanding of how cyberspace intersects with global politics.

State-Sponsored Cyber Attacks

State-sponsored cyber-attacks refer to cyber-attacks that are initiated or supported by governments to achieve specific political, economic, or military objectives (Waltz, 2019). These attacks are characterized by their sophistication, stealth, and persistence, with state-sponsored attackers often employing advanced techniques and tools to evade detection and attribution (Singer & Friedman, 2014). State-sponsored cyber-attacks can target a wide range of entities, including critical infrastructure, government agencies, and private companies, and can have significant economic, political, and security implications (Lindsay, 2018).State-sponsored cyber-attacks, also known as cyber-enabled espionage, refer to the use of digital tools and techniques by governments or state-affiliated actors to gain unauthorized access to sensitive information or computer systems belonging to individuals, organizations, or other states. These attacks are characterized by the use of sophisticated and often stealthy techniques such as malware, phishing, and social engineering to compromise the target systems or networks, and the theft of sensitive data, intellectual property, or strategic information for political, economic, or military gain (Kshetri, 2017; Lewis, 2018).

One of the primary motivations for state-sponsored cyber-attacks is to gain a strategic advantage over other countries or actors in the international arena. These attacks can be used to undermine the security and stability of other nations, disrupt critical infrastructure, or steal sensitive information that can be used for economic or military purposes (Rid, 2012). For instance, China's APT10 hacking group has been accused of targeting several companies and organizations in the United States, stealing trade secrets and intellectual property worth billions of dollars (Department of Justice, 2018).Another characteristic of state-sponsored cyber-attacks is the use of deniability and deception to mask the identity of the attacker. Governments often use third-party actors, such as criminal syndicates or hacktivist groups, to carry out attacks on their behalf, making it difficult to attribute responsibility for the attack (Janczewski & Colarik, 2014). This allows states to pursue their strategic objectives without facing diplomatic or military consequences for their actions.

Furthermore, state-sponsored cyber-attacks are becoming increasingly prevalent and sophisticated. The development of advanced tools and techniques, such as zero-day exploits, artificial intelligence, and machine learning, has enabled attackers to launch more targeted and effective attacks (Council of Europe, 2018). For instance, the Stuxnet worm, believed to have been developed by the United States and Israel, was specifically designed to target and sabotage Iranian nuclear facilities, causing significant damage to the country's nuclear program (Greenwald & MacAskill, 2012).

Policy Approaches and Strategies Adopted by Countries and International Organizations

Scholars have offered various opinions on the key policy approaches and strategies adopted by different countries and international organizations to address cybersecurity issues in the realm of international politics from 2010 to 2023 and reasons behind these approaches and strategies include:

National Cybersecurity Strategies

Many countries have developed national cybersecurity strategies to protect their critical infrastructure and national interests. These strategies typically involve a combination of legislative measures, capacity building, and public-private partnerships. Smith and Young (2017) highlight that "countries like the United States and the United Kingdom have adopted comprehensive national cybersecurity strategies, emphasizing public-private cooperation and threat information sharing."

International Cooperation and Agreements
International cooperation is a central theme in addressing cybersecurity issues. Scholars like Rosenzweig (2018) argue that international agreements and organizations play a crucial role. For instance, the Budapest Convention on Cybercrime has facilitated cooperation among countries in investigating and prosecuting cybercrimes.

Offensive Cyber Capabilities
Some countries like Russia and North Korea have developed offensive cyber capabilities as part of their cybersecurity strategies. Rid and McBurney (2012) discuss the controversial issue of "active defense" or "hack back" strategies, where states retaliate against cyber attackers. Such strategies raise ethical and legal concerns but are viewed by some as a deterrent.

Public-Private Partnerships
Public-private partnerships have gained prominence in addressing cyber threats. Scholars like Libicki (2017) argue that collaboration between governments and private sector entities is essential. Initiatives like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) emphasize cooperation with the private sector to enhance cybersecurity.

Cyber Deterrence and Attribution
The concept of cyber deterrence has been debated extensively. Braw (2018) suggests that countries are exploring ways to deter cyber adversaries through a combination of offensive capabilities, declaratory policies, and attribution efforts to hold perpetrators accountable notable among countries that have adopted this strategy is China.

Norms Development
Efforts to develop norms of responsible state behavior in cyberspace have been ongoing. Talbot and Jensen (2017) discuss the role of the United Nations Group of Governmental Experts (UN GGE) in establishing norms for responsible state behavior in cyberspace.

Capacity Building and Cybersecurity Education
Scholars such as Clarke and Knake (2019) argue that capacity building and cybersecurity education are essential components of national strategies. These initiatives aim to develop a skilled workforce capable of defending against cyber threats, and the US has invested heavily on this approach.

Cybersecurity Governance and Regulation
Many countries have introduced regulatory frameworks to enhance cybersecurity in critical sectors. Talbot (2016) notes that regulations often require organizations to implement cybersecurity measures and report incidents.

State-Sponsored Cyber Attacks 2010-2023
Several case studies have highlighted the impact of state-sponsored cyber-attacks on international relations and national security.
The 2014 Sony Pictures hack, for instance, was attributed to North Korea and was seen as retaliation for the release of a film that portrayed the country's leader in a negative light (Watts, 2018). The attack resulted in significant financial and reputational damage to Sony Pictures and led to a diplomatic row between the U.S. and North Korea. Another case is the 2017 NotPetya attack, which was attributed to Russia and was seen as a response to Ukraine's efforts to sever its ties with Russia (Lakin & Roze, 2018). The attack disrupted critical infrastructure in Ukraine and caused significant economic damage to several global companies.

According to a report by the Center for Strategic and International Studies (2020), African countries have been frequent targets of both state-sponsored and criminal cyber-attacks. For instance, the cyber-attack on the Democratic Republic of Congo's electoral commission in December 2018, which was believed to

be an attempt to disrupt the country's presidential elections, was attributed to a group of hackers with ties to Russia (Center for Strategic and International Studies, 2020). Similarly, in 2020, a Chinese advanced persistent threat group carried out a cyber espionage campaign called "Operation North Star" that targeted several African countries, including Egypt, Sudan, and Uganda (Center for Strategic and International Studies, 2020). This suggests that state-sponsored cyber-attacks can have significant implications for political stability and national security in African countries. In addition to state-sponsored attacks, African countries have also been targeted by cybercriminals, as evidenced by the 2019 bank heist in West Africa, which resulted in the theft of millions of dollars from banks in Ghana and Nigeria (Center for Strategic and International Studies, 2020). These incidents highlight the need for effective cyber security measures to protect against both state-sponsored and criminal cyber threats. Another significant state-sponsored cyber-attacks is the Stuxnet cyber-attack which targeted Iran's nuclear facilities and is widely believed to have been developed and launched by a joint operation between the United States and Israel. The primary motivation behind the Stuxnet attack was to disrupt Iran's nuclear program, particularly its uranium enrichment efforts. Iran's pursuit of nuclear capabilities had raised concerns within the international community about potential weapons development. The United States, in collaboration with Israel, sought to impede Iran's progress towards a nuclear weapon by targeting its nuclear infrastructure. The technical objectives are to Sabotage Industrial Control Systems. Stuxnet was a highly sophisticated malware designed to specifically target and sabotage industrial control systems, particularly those used in Iran's Natanz uranium enrichment facility.

The attackers aimed to manipulate the centrifuges' operation by altering their rotational speeds, leading to physical damage and hindering Iran's uranium enrichment process. Another one is the Covert Strategy - Maintaining Deniability, the United States, along with Israel, allegedly employed a covert strategy to develop and launch the Stuxnet attack. The attack was designed to remain undetectable for as long as possible, ensuring plausible deniability. By using various techniques, such as the exploitation of zero-day vulnerabilities and sophisticated obfuscation methods, the attackers aimed to prevent attribution of the attack to their respective governments. The Stuxnet attack marked a significant escalation in cyber warfare tactics. It demonstrated that cyber operations could be used as a powerful tool to disrupt critical infrastructure and sabotage key targets. The attack also exposed vulnerabilities in industrial control systems, highlighting the need for enhanced cyber-security measures in critical sectors worldwide (CSIS, 2023).

May 2023: Belgium’s cyber security agency has linked China-sponsored hackers to aspear fishing attack on a prominent politician. The attack comes as European governments are increasingly willing to challenge China over cyber offences. May 2023: Chinese hackers breached communications networks at a U.S. outpost in Guam. The hackers used legitimate credentials, making it harder to detect them.
May 2023: Chinese hackers targeted Kenyan government ministries and state institutions, including the presidential office. The hacks appeared to be aimed at gaining information on debt owed to Beijing.
December 2022. Microsoft reported that it observed a pattern of attacks targeting Ukrainian critical infrastructure from Russian hacking group, Sandworm. These attacks were accompanied by pro-Russian propaganda.

December 2022. Russia-linked hackers launched a DDoS attack against Vatican City servers, knocking its official website offline. The attack came three days after Russian government officials criticized Pope Francis for his comments about the war in Ukraine.

December 2022. Chinese government-linked hackers stole at least $20 million in COVID-19 relief funds from the U.S. government, including Small Business Administration loans and unemployment insurance money. The U.S. Secret Service announced they retrieved half of the stolen funds thus far.
September 2021. In April 2020, Chinese bots swarmed the networks of the Australian Center for Strategic and International Studies (CSIS) | Washington, D.C. government days after Australia called for an

independent international probe into the origins of the corona virus. These bots looked for potential vulnerabilities on the network to exploit in future cyber-attacks.

August 2021. A cyber-espionage group linked to one of Russia's intelligence forces targeted the Slovak government from February to July 2021 through spear-fishing attempts.
August 2021. Russia targeted and blocked content on "smart voting" app created by Kremlin critic Alexei Navalny and his allies intended to organize voting against the Kremlin in next month's parliamentary elections.

December 2020. North Korean hackers targeted U.S. pharmaceutical companies Johnson Johnson and Novavax, both working on experimental vaccines.

December 2020. African Union staff found that Chinese hackers had been siphoning off security footage from cameras installed in the AU headquarters.

December 2020. Facebook found that two groups of Russians and one group of individuals affiliated with the French military were using fake Facebook accounts to conduct dueling political information operations in Africa.

December 2019. Iranian wiper malware was deployed against the network of BAPCO, the national oil company of Bahrain.

December 2019. Russian government hackers targeted Ukrainian diplomats, government officials, military officers, law enforcement, journalists, and nongovernmental organizations in a spear phishing campaign.

October 2019. An Israeli cybersecurity firm was found to have sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in Whatsapp.

December 2018. The United States, in coordination with Australia, Canada, the UK, and New Zealand, accused China for conducting a 12-year campaign of cyber espionage targeting the IP and trade secrets of companies across 12 countries. The announcement was tied to the indictment of two Chinese hackers associated with the campaign.

December 2018. U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.

November 2018. German security officials announced that a Russia-linked group had targeted the email accounts of several members of the German parliament, as well as the German military and several embassies.

October 2017. Reports surface that Russian government-backed hackers stole NSA hacking secrets from a contractor in 2015 by exploiting the Kaspersky antivirus software on the contractor's home computer.

September 2017. An Iranian hacking group was responsible for an espionage campaign targeting the aerospace industry in the U.S. and Saudi Arabia, as well as petrochemical firms in South Korea and Saudi Arabia.

July 2017. Russian hackers used leaked NSA tools to compromise Wi-Fi servers in European and Middle Eastern hotels in a campaign targeting top diplomats and industrial leaders.

December 2016. Russian hackers targeted Ukraine's national power company, UKRENERGO, and shut down power to northern Kiev for over an hour.

October 2016. The U.S. Director of National Intelligence and Department of Homeland Security jointly identified Russia as responsible for hacking the Democratic National Committee and using Wiki Leaks to dump emails obtained in the hack.

August 2016. Brazilian hackers ramped up phishing attacks against tourists visiting Rio de Janeiro for the 2016 Olympics. Security researchers ranked Brazil second only to Russia in the sophistication of its financial fraud gangs.
December 2015. Russian hackers coordinated attacks on several regional power distribution companies in Western Ukraine. SCADA systems and system host networks were targeted and damaged. Malware was used to probe for network vulnerabilities, establish command and control, and wipe SCADA servers to delay restoration. Attackers simultaneously launched a denial of service attack on system dispatchers to prevent customers from reporting disruptions. Approximately 225,000 Ukrainians were affected, but service was restored after 3-6 hours.

November 2015. Iran's Revolutionary Guard hacked the email and social media accounts of a number of Obama administration officials in attacked believed to be related to the arrest of an Iranian-American businessman in Tehran.

July 2015. A spear phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel. Officials believe that Russia is responsible for the intrusion, which occurred sometime around July 25, although China has not been ruled out as the perpetrator.

December 2014. Iranian hackers attacked a major Las Vegas casino in retaliation for its owner's support for Israel.

December 2014. An Iranian cyber campaign targeted government agencies and critical infrastructure companies in the United States, Canada, Europe, the Middle East, and Asia.

October 2014. A five-year cyber espionage campaign attributed to Russia exploits a zero-day vulnerability in Windows software on computers used by NATO, the EU and the Ukrainian government. *All the above records are from (Center for Strategic and International Studies (CSIS) | Washington, D.C. 2023).

Theoretical Framework

There are various theories on state behavior in cyberspace, with some scholars arguing that cyberspace represents a new domain of conflict and competition between states (Libicki, 2017). Realist scholars, for instance, contend that states seek to gain power and influence in cyberspace, just as they do in other domains, and that competition among states is inevitable (Mearsheimer, 2019). Others argue that cyber-attacks can be used as a means of coercion, with states using cyber capabilities to achieve specific political objectives (Mazanec, 2016). Constructivist scholars, on the other hand, emphasize the role of norms and values in shaping state behavior in cyberspace, arguing that the development of a shared understanding of the norms and rules governing cyberspace is essential to promote stability and security (Finnemore & Sikkink, 2019).

To determine which theoretical framework can best analyze this research topic, it is necessary to consider the specific research question and context. However, one framework that has been commonly used in the study of cybersecurity that properly explains why states pursue cyber security policy is the theory of Securitization, developed by the Copenhagen School in the 1990s (Buzan, Waever, & De Wilde, 1998).

According to the securitization theory, security threats are not objective, but rather are constructed through the actions of political actors who seek to frame certain issues as existential threats that require exceptional measures. This process of securitization can lead to the prioritization of certain policy issues, the marginalization of certain groups, and the erosion of civil liberties (Wæver, 2011).This paper adopted securitization theory as our framework, and it is useful for analyzing cybersecurity, as it highlights how the framing of cyber security threats as existential risks can have significant political and social consequences. For example, governments may use the language of cyber security to justify increased

surveillance or censorship, or to justify military interventions in other countries. Critics of the securitization framework argue that it can be overly deterministic and neglect the agency of non-state actors in shaping security dynamics.

Others argue that the theory can be too narrow in its focus on traditional security threats and may neglect other important dimensions of security, such as economic or environmental security (McDonald & Valeriano, 2016). In our research topic "cyber security and international conflict: an analysis of state-sponsored cyber-attacks", securitization theory becomes suitable because it explains that states involves in the use of cyber-attacks as a means of national security policy which give them leverage of supremacy over other states. Example is in 2015, when Russian hackers alleged sponsored by Russian state coordinated attacks on several regional power distribution companies in Western Ukraine. SCADA systems and system host networks were targeted and damaged. Malware was used to probe for network vulnerabilities, establish command and control, and wipe SCADA servers to delay restoration. Attackers simultaneously launched a denial of service attack on system dispatchers to prevent customers from reporting disruptions. Approximately 225,000 Ukrainians were affected, but service was restored after 3-6 hours, major reason is to among other things intimidate Ukraine and cause them multi-million dollar damages.

Research Methodology

An extensive review of scholarly articles, books, and reports related to cyber security and international politics from 2010 to 2023 was conducted as the foundational step to identify the key issues, trends, and theoretical frameworks relevant to the subject matter. Official government documents, policy statements, and international agreements related to cyber security and international politics was also systematically analyzed. Historical and content analysis was also employed in order to explore the trends in cyber security and international politics over the specified period and what scholars have done in this regard over the period of time under study. This analysis involved tracing the evolution of cyber threats, international responses, and diplomatic interactions to identify patterns, shifts, and changes that have occurred in this domain.

Factors Contributing to State-Sponsored Cyber Attacks

The analysis of secondary data sources revealed that there are several factors contributing to state-sponsored cyber-attacks. These factors include economic and political interests, national security concerns, and technological capabilities. For example, China's Operation North Star, a cyber espionage campaign that targeted several African countries in 2020, was believed to have been carried out to gain a competitive advantage in the global market.

Comparative Analysis of State-Sponsored Cyber Attacks in Different Regions

The comparative analysis of secondary data sources revealed that state-sponsored cyber-attacks differ in their targets, methods, and motivations depending on the region. For example, in the Middle East, state-sponsored cyber-attacks have been used to target critical infrastructure, while in East Asia, cyber-attacks have been used to steal intellectual property.

Discussion of Findings

The analysis of secondary data sources provided a comprehensive understanding of state-sponsored cyber-attacks and their implications for international conflict. The findings suggest that state-sponsored cyber-attacks are a growing threat to international security and require concerted efforts by the international community to address them. The research also highlights the need for more research to understand the dynamics of state-sponsored cyber-attacks and to develop effective strategies to mitigate their impact. State-sponsored cyber-attacks, which are carried out by governments or state-sponsored actors for various reasons, have become a growing concern in the field of cyber security (Smith, 2019). These attacks can result in the theft of sensitive information, disruption of critical infrastructure, or political instability in other countries (Johnson & Smith, 2018). State-sponsored cyber-attacks have

become more sophisticated and widespread over the past decade (Jones & Lee, 2020). The global nature of these attacks poses a significant threat to the security and stability of the international community.

State-sponsored cyber-attacks can be defined as those that are backed by a government or state entity, whether through direct involvement or by providing resources and support to a non-state actor (Smith, 2019). The attacks are aimed at achieving economic and political interests, national security concerns, or technological capabilities. State-sponsored cyber-attacks are difficult to detect and mitigate, as they often involve sophisticated methods and techniques. In 2020, there was a significant increase in state-sponsored cyber-attacks, with various countries and organizations being targeted (Jones & Lee, 2020). These attacks ranged from espionage and data theft to disruption of critical infrastructure and political interference. The Stuxnet worm is one of the notable examples of state-sponsored cyber-attacks, which was developed by the United States and Israel and used to target Iran's nuclear program (Zetter, 2015). The attack demonstrated the potential for state-sponsored cyber-attacks to cause physical damage to critical infrastructure. Another example is the 2014 cyber-attack on Sony Pictures, which was attributed to North Korea and aimed at disrupting the release of a film that portrayed the country's leader in a negative light (Zetter, 2015).

State-sponsored cyber-attacks pose a significant threat to cyber security as they have the potential to cause significant damage to critical infrastructure, disrupt economies, and compromise sensitive information (Johnson & Smith, 2018). The lack of effective detection and mitigation strategies for such attacks makes them even more dangerous (Smith, 2019).Several factors contribute to state-sponsored cyber-attacks, including economic and political interests, national security concerns, and technological capabilities (Johnson & Smith, 2018). In some cases, state-sponsored cyber-attacks are carried out to gain a competitive advantage in the global market, while in others, they are aimed at disrupting the political stability of other countries (Smith, 2019).

The international community has developed various strategies to mitigate the impact of state-sponsored cyber-attacks, including developing international norms and standards for cyber security, enhancing cooperation between countries, and improving cyber defenses (Jones & Lee, 2020). The use of sanctions and diplomatic measures has also been used to deter state-sponsored cyber-attacks (Johnson & Smith, 2018).Despite the efforts to mitigate the impact of state-sponsored cyber-attacks, there are still several challenges that need to be addressed. One of the main challenges is the lack of a unified approach to cyber security, with different countries having different perspectives and priorities (Smith, 2019). The difficulty in attributing cyber-attacks to a specific state or actor is also a significant challenge (Jones & Lee, 2020).In conclusion, state-sponsored cyber-attacks pose a significant threat to cyber security and the stability of the international community. It is essential to develop effective strategies to mitigate their impact, including developing international norms and standards for cyber security, enhancing cooperation between countries, and improving cyber defenses. Addressing the challenges associated with state-sponsored cyber-attacks is crucial to ensuring a secure and stable cyberspace for all (Johnson & Smith, 2018).

Conclusion

Our study shows that state-sponsored cyber-attacks have become a significant threat to cyber security and the stability of the international community. The global nature of these attacks requires a concerted effort by the international community to develop effective strategies to mitigate their impact. We have identified several factors contributing to state-sponsored cyber-attacks, including economic and political interests, national security concerns, and technological capabilities. In addition, we have highlighted the challenges associated with mitigating the impact of these attacks, including the lack of a unified approach to cyber security and the difficulty in attributing cyber-attacks to a specific state or actor. In this research, we have explored the global overview of state-sponsored cyber-attacks and their implications for cyber security. We have discussed the definition of state-sponsored cyber-attacks, provided an overview of

such attacks, and highlighted some notable examples. We have also examined the factors contributing to state-sponsored cyber-attacks and identified the challenges in mitigating their impact.

Recommendations

Based on our analysis, we recommend that governments and international organizations take the following steps to enhance cyber security and mitigate the impact of state-sponsored cyber-attacks:

1. Develop international norms and standards for cyber security: International norms and standards for cyber security can help establish a shared understanding of cyber threats and promote cooperation among countries in addressing these threats.
2. Enhance cooperation between countries: Improved cooperation between countries can facilitate the sharing of information and resources, enabling a more effective response to state-sponsored cyber-attacks. Again governments and organizations should enhance their cyber defenses, including investing in advanced technologies and developing robust incident response plans.
3. Use sanctions and diplomatic measures: The use of sanctions and diplomatic measures can be an effective way to deter state-sponsored cyber-attacks and hold those responsible accountable for their actions. Also governments and international organizations should work towards developing a more unified approach to attribution, which would make it easier to hold those responsible for state-sponsored cyber-attacks accountable.

Finally, state-sponsored cyber-attacks pose a significant threat to cyber security and the stability of the international community. Governments and international organizations must take a proactive approach to enhance cyber security and mitigate the impact of such attacks. By developing international norms and standards, enhancing cooperation, improving cyber defenses, and addressing the challenges associated with attribution, we can create a more secure and stable cyberspace for all.

References

Arquilla, J. (2017). Cyber Swarming and the Future of War. Foreign Affairs, 96(6), 34-41.

Buzan, B., Waever, O., & De Wilde, J. (1998). Security: A new Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.

Center for Strategic and International Studies (CSIS). (2023). Significant Cyber Incidents. Retrieved from https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Center for Strategic and International Studies (CSIS). (2020). Significant Cyber Incidents. Retrieved from https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Council of Europe. (2018). Cybercrime and Cyber-related Offences. Council of Europe. Retrieved from https://www.coe.int/en/web/cybercrime/cybercrime-and-cyber-related-offences

Choucri, N., & Clark, D. (Eds.). (2018). Cyber Security and Geopolitics: National Security Imperatives. Springer.

Council of the European Union. (2017). Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defense: Building Strong Cybersecurity for the EU. Brussels, 13.9.2017. COM (2017) 477 final.

Deibert, R. J., & Rohozinski, R. (2010). Beyond Denial: Introducing Next-Generation Information Access Controls. First Monday, 15(11).

Department of Justice. (2018, December 20). Chinese Hackers Associated with Ministry of State Security charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information. United States Department of Justice. Retrieved from https://www.justice.gov/opa/pr/chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Finnemore, M., & Sikkink, K. (2019). International Norm Dynamics and Political Change. Oxford University Press.

Gartzke, E., & Lindsay, J. R. (2019). The Information Revolution in Military Affairs. International Security, 43(1), 141-179.

Greenwald, G., & MacAskill, E. (2012, June 1). Revealed: How the World's First Cyber Weapon Affected Iran's Nuclear Programme. The Guardian. Retrieved from https://www.theguardian.com/world/2012/jun/01/stuxnet-worm-iran-nuclear-programme

Janczewski, L. J., & Colarik, A. M. (Eds.). (2017). Cyber Warfare and Cyber Terrorism. Springer.

Jones, K., & Lee, M. (2020). State-Sponsored Cyber Attacks: An Overview. Journal of Computer Security, 28(3), 235-252. doi: 10.3233/JCS-190096

Johnson, T. A., & Smith, R. B. (2018). Factors Contributing to State-Sponsored Cyber Attacks. Journal of Cybersecurity, 3(2), 103-120. doi: 10.1093/cybsec/tyy014

Krekel, B., et al. (2021). State-Sponsored Cyber Operations and International Politics: Implications for Security and Conflict. International Studies Quarterly, 65(1), 58-71.

Kshetri, N. (2017). Block Chain's Roles in Meeting Key Supply Chain Management Objectives. International Journal of Information Management, 37(2), 1-9. https://doi.org/10.1016/j.ijinfomgt.2016.11.007

Lewis, J. A. (2018). The Attribution Problem in Cyberspace. In J. S. Forrest, & A. M. Collins (Eds.), Cyber security and Politics: The Psychological and Institutional Dimensions (pp. 39-54). Routledge.

Nye, J. S. (2015). The Regime Complex for Managing Global Cyber Activities. Global Governance, 21(1), 17-22.

McDonald, M. P., & Valeriano, B. (2016). Cyber Security and Critical Infrastructure Protection. New York: Springer.

Ollivant, D. (2016). Between a Cyber Rock and a Hard Place: The Economic and Technological Implications of Government Offensive Cyber Capabilities. Survival, 58(1), 7-32.

Rid, T. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32. https://doi.org/10.1080/01402390.2011.608939

Rid, T., & Buchanan, B. (2019). Attributing Cyber Attacks. Journal of Strategic Studies, 42(6-7), 491-525.

Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Smith, R. B. (2019). Understanding State-Sponsored Cyber Attacks. Journal of Cybersecurity, 4(1), 12-27. doi: 10.1093/cybsec/tyz004

Wæver, O. (2011). Securitization and De-Securitization. In T. Balzacq (Ed.), Securitization Theory: How Security Problems Emerge and Dissolve (pp. 46-86). London: Routledge

Zetter, K. (2015). The Rise of State-Sponsored Cyber Attacks. Wired. Retrieved from https://www.wired.com/2015/06/rise-state-sponsored-cyberattacks/

Author's Biography

Azubuike Callistus Francis is a Lecturer in the Department of Political Science Nnamdi Azikiwe University, Awka Anambra State Nigeria. He holds M.Sc in Political Science (International Relations) from Nnamdi Azikiwe University. He has a strong research background in International Political Economy, Global Conflicts, Migration and Refugee related issues and Elections and Corruption on Africa's Political Dynamics. In addition to his research contributions, Azubuike Callistus Francis is actively engaged in teaching or mentorship roles, educating the next generation of researchers and scientists. His current research interests include: British exit from EU and its impact on British Economy; Climate Change and Migration Patterns He is committed to broadening the understanding of Africa's global engagements in the global politics of Nations; provide critical researched information on Africa's socio-political and economic global involvements, and how Africa will be major players on global politics and global decisions.