IJEMD-SS, 3 (1) (2024), 1 –8 https://doi.org/10.54938/ijemdss.2024.03.1.347

IJEMD

International Journal of Emerging Multidisciplinaries:
Social Science

Research Paper
Journal Homepage: www.ojs.ijemd.com
ISSN (print): 2957-5311 ISSN (online): 2958-0277

Cyberwarfare and Arms Control: Analyzing the SolarWinds Hack of 2020

Bala Iranyang Shamaki [1*], Anthony Ebere Shalom[1] , Oyinu Egahi Junior[1] , Yaweh Filibus[2]

1.Department of Political Science, Federal University Wukari-Nigeria.

2.Department of History and Diplomatic Studies , Federal University Wukari-Nigeria

Abstract

This research examines the implications of cyber warfare on international arms control, particularly in light of the SolarWinds hack, a pivotal event explaining the vulnerabilities in our increasingly digital world. Dependency on cyberspace has rendered states susceptible to emerging threats, while existing arms control treaties, relics of the Cold War, have failed to adapt to contemporary realities. Employing an ex post facto research design, this study utilizes secondary data analysed through content analysis, grounded in Realism theory as the analytical framework. The findings reveal the multifaceted challenges posed by cyber warfare, including issues of attribution, pervasive mistrust among nation-states, economic repercussions, attacks on critical infrastructure, and intensified international rivalries. The SolarWinds hack serves as a case study that underscores the urgent need for modernizing arms control regimes to address these new dynamics. The study concludes that without proactive adaptations in international security frameworks, the risks associated with cyber warfare will continue to escalate, jeopardizing global stability and undermining cooperative efforts to ensure a secure future. This research calls for a re-evaluation of arms control in the context of cyber threats, emphasizing the necessity for innovative strategies to enhance resilience and promote trust among states.

Keywords: Cyberwarfare, Arms Control, SolarWinds Hack, National Security, State-sponsored Attacks.

Introduction

The rapid increase in internet use has radically transformed communication among states, non-state actors, corporations, universities, and individuals resulting in an escalating dependence on computer systems and

Email Addresses: yaweh@fuwukari.edu.ng **(Yaweh),** egahioyinu@gmail.com **(Oyinu),** shallytony14@gmail.com **(Anthony),** balaira2013@gmail.com **(Bala).**

networks. This dependency has led to the emergence of cyberspace as a new battlespace now recognized as the fifth domain of warfare alongside land, sea, air, and space [47]. Yet, this digital battlefield brings enormous vulnerabilities as evidenced by the 2020 SolarWinds hack, which exposed glaring security gaps and the inadequacies of traditional arms control treaties in addressing cyber threats.

Cyberspace provides essential opportunities but remains highly susceptible to malicious activities, facilitating intense competition among global powers. Cyber warfare tactics now range from cyber espionage and interference with command-and-control systems to targeting critical national infrastructure, including nuclear systems. Unlike traditional warfare, cyber warfare crosses borders and operates without clear-cut physical boundaries, creating distinctive challenges in regulation and enforcement [48] Former U.S. President Barack Obama pointed out cyber threats as among the most pressing economic and national security issues of the 21st century [32], [48] a sentiment that underscores the critical need for states to re-evaluate their cyber defences and strategies. Major powers are responding with unprecedented investments; for example, the UK plans to allocate €2 billion, and France, the UAE, and Australia each plan to commit around €1 billion to their cybersecurity frameworks [11].

However, as cyber risks intensify, arms control efforts lag, leaving states vulnerable to cyber warfare escalation. The frequency of state-sponsored cyber-attacks has risen by 60% over the past six years with China, Russia, Iran, and North Korea among the top perpetrators. These state-backed cyber operations are destabilizing international relations, disrupting critical infrastructure, and threatening national security [4] [16]. With cyberweapons capable of undermining economic stability, manipulating political processes, and threatening human rights, the stakes of cyber warfare are unparalleled. Yet, unlike conventional arms control, the regulation of cyber capabilities remains poorly defined. Arms control treaties that were created during the Cold War are now outdated, failing to address the complexity and speed of contemporary cyber conflicts.

One of the greatest challenges in cyber arms control is adapting existing frameworks to the intangible nature of cyberspace. Traditional arms control treaties govern state operations concerning physical weapons, yet applying these agreements to cyber warfare is complex due to its distinct properties. Without defined norms and agreements in cyberspace, the potential for cyber arms races and escalations increases, further endangering international stability. This article explores the need for innovative arms control approaches tailored to cyberspace by examining the SolarWinds hack as a case study.

Conceptual Clarification

The Concept of Cyberwarfare

According to the Tallin Manual on the International Law Applicable to Cyberwarfare, Cyberwarfare involves the use of cyber operations to cause harm or damage to an adversary's computer systems, networks or infrastructure. It is conducted by states actors, or organized criminal groups to achieve

strategic or tactical objectives [44]. Cyber warfare can be defined as an activity of units, institutions, state or non-state actors or well-trained individuals operating within cyberspace using computer-related assets and infrastructure to conduct offensive and defensive operations [15].

Cyberwarfare can also be defined as a criminal intent conducted by state or non-state actors using computers to attack digital infrastructure or obstruct other computers or networks within cyberspace for malicious, political, religious, military, economic or strategic motives [22].

The Concept of Arms Control

Arms Control is a "unilateral measures, bilateral and multilateral agreements as well as informal regimes between States to limit or reduce certain categories of weapons or military operations in order to achieve stable military balances and thus diminish tensions and the possibility of large-scale armed conflict" [9].

[36] define arms control as having three principal tasks: to prevent or reduce the likelihood of conflict breaking out; to limit the damage caused by these weapons in the event of conflict; and to reduce the cost of producing weapons and free up these funds for other projects. Arms control can take many forms, including treaties, agreements, and international laws. It assumes that rivalry between states will continue to exist, as will military potential. Therefore, arms control is not about total elimination, but about monitoring the number, production, development, storage of weapons, and deployment of troops.

Empirical Review

The empirical review compellingly argues that the interplay between cyber warfare and arms control necessitates urgent attention in contemporary security discussions. [25] contend that existing verification mechanisms and confidence-building measures from traditional arms control frameworks such as the Conventional Forces in Europe Treaty and the Open Skies Treaty can serve as valuable blueprints for a cyber-domain arms control regime. They assert that establishing a trust-based framework, underpinned by robust verification methods, is germane for effectively mitigating the multifaceted threats posed by cyber actors.

[8] further amplifies this argument by highlighting the gigantic risks associated with the arms race in cyberspace. He criticizes the inadequate emphasis on arms control in international cybersecurity dialogues, despite its pivotal role in maintaining global stability. [8] underscores the necessity of collaboration among diverse stakeholders—political actors, multilateral organizations, and civil society—to forge a comprehensive regulatory framework for cyberspace.

Adding to this discourse,[3] illuminates the alarming rise in state-sponsored cyber-attacks driven by an ever-increasing reliance on technology. He argues that the motivations behind these attacks ranging from economic interests to national security concerns demand a multifaceted response that combines diplomatic, legal, and technical measures. The call for international norms to facilitate cooperation is not merely theoretical; it is a pressing necessity for safeguarding global security in an interconnected world.

[5] contributes to this narrative by illustrating the transformative nature of cyber warfare in modern conflicts. His historical analysis reveals how the evolution of cyber tactics has reshaped state behavior and the terrain of international relations. The implications are enormous: if left unaddressed, cyber threats could destabilize the very foundations of global security.

[10] reinforces the argument by asserting that national security is increasingly jeopardized by sophisticated cyber warfare tactics targeting military capabilities and critical infrastructure. The frequent and devastating nature of these cyberattacks necessitates robust mitigation strategies. This urgency highlights the vital need for comprehensive cybersecurity strategies, global collaboration, and enhanced information-sharing initiatives to counteract the insidious risks posed by cyber warfare and espionage.

Theoretical Framework

Realism Theory is adopted as the theoretical framework for this research. Realism theory in international relations emphasizes the state as the principal actor in the anarchical international system and must pursue their national interest for survival and maintenance of power and security and that they will use any means to achieve it [51], [28].

The SolarWinds hack case have received attention in regard to cyberwarfare. The hack has been attributed to Russia against the United States. Cyberwarfare has become an emerging threat in the international system and can be used as tool of state to pursue their interest without using traditional military force. From the realist point of view, the SolarWinds hack is seen as Russia attempts to gain strategic advantage by in infiltrating and gathering intelligence from United States government agencies and private sector companies. This suggests that Russia is motivated to pursue her national interest and undermine the security of other states. [51] stated that state must be concerned about the capabilities of other states. States are making choices to increase their capabilities while undermining the capabilities of others, Russia's sophisticated cyber operation, which penetrated major United States institutions, demonstrates its cyber capabilities and potential to influence and destabilize adversaries (Valeriano, Jensen & Maness, 2018), showcasing its power and influence as the struggle for power is universal in time and space [28].

The response of the United States by imposing sanctions and expelling Russian diplomats stems from its national interest in maintaining power and security. The cyber warfare against the United States will further compel it to prioritize cybersecurity in its national security agenda, focusing on strengthening defenses, improving threat intelligence, and enhancing agency coordination.

From the realist perspective, [51] stated the anarchic nature of the international system causes nations to compete against one another. The cyberwarfare (The SolarWinds hack) has strained the relations between the United States and Russia. In applying realism theory, when a state survival is threatened by a state or coalition of stronger state, it should establish a formal alliance and seeks to preserve its survival by checking the owe of opposing states [51]. In order to curb the emerging threat of cyberwarfare, there is a need for international norms, law, cooperation and enforcement in order to mitigate, manage the threat.

An Overview of the SolarWinds Hack 2020

SolarWinds is a large and reputable U.S information technology (IT) company founded in 1999, headquartered in Texas [19], [24].SolarWinds provides network performance and system monitoring software that enables businesses to identify, diagnose, and solve critical networking and IT problems. It develops software for top organizations to manage their network systems and information technology infrastructure [23]. The SolarWinds Orion platform has access to customer system performance logs and data. It is used by over 300,000 customers worldwide, including telecom companies, military and government organizations such as the Pentagon, the United States Aeronautics and Space Administration (NASA), and the National Security Agency (NSA) among others [30].

The United States suffered the biggest cyber-attack ever in terms of sophistication and extent of impact in 2020 [47]. The SolarWinds hack was a "supply chain" type of operation in that it vectored malware through updates of the Orion software product of SolarWinds, which is widely used to manage IT resources along business supply chains. The malicious code creates a backdoor to customers' systems, which enables hackers to install more malware and to spy on their victims [24].

[21], Perlroth, and [44] stated that the attack was carried out by APT29, a Russian espionage group known as Cozy Bear, which is known for targeting global government, diplomatic, and commercial entities. APT29 is believed to be the primary threat actor behind the SolarWinds hack. The scale of the attack has led analysts to consider it one of the most sophisticated in the nation's history and one of the biggest cybersecurity breaches of the 21st century, with some tagging it as a national security threat[47], [33].This serious large-scale attack on SolarWinds has signaled the possibility of cyber warfare becoming more present and intense than ever before. SolarWinds stated that up to 18,000 out of more than 300,000 of its customers were infected with malicious code [47], [43].

Table 1 The SolarWinds hack timeline

S/no	Date	Events
1.	September 4, 2019	Threat actors gain unauthorized access to SolarWinds network
2.	October 2019	Threat actors test initial code injection into Orion
3.	February 20, 2020	Malicious code known as Sunburst injected into Orion
4.	March-June; 2020	SolarWinds unknowingly starts sending out Orion software updates with hacked code as victims downloaded malicious software
5.	June-December 2020	Follow up attacks on selected victims began. Threat actors exploited the SUNBURST backdoor to gain persistent access to various organizations' networks, conduct reconnaissance, and extract sensitive information
6.	December 8, 2020	FireEye, a cybersecurity firm reported a breach and theft of its red team tools, following a breach in the SolarWinds supply chain.
7.	December 13, 2020	FireEye and SolarWinds disclosed a supply chain attack, prompting the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to issue an emergency directive for federal agencies.

8.	December 2020	Investigations revealed compromised federal agencies like Treasury, Commerce, and Homeland Security, as well as major technology companies and critical infrastructure organizations.
9.	January 2021	The U.S. government initially linked the attack to a nation-state actor, later identifying it as likely being Russian intelligence services, specifically APT29 or Cozy Bear.
10.	February 2021	The cleanup and remediation efforts continued, focusing on removing malicious code, enhancing security measures, and thoroughly investigating the extent of the breach.

Source; [41], [33].

[41] and [47] outlined the government agencies attacked which are; The Pentagon; The United States of Aeronautics and Space Administration (NASA); The Department of Homeland Security; The Department of State; The Department of Commerce; The Department of Defense; The Federal Bureau of Investigation. The major companies targeted are; Microsoft; Intel; Cisco; VMware and FireEye. [49], [7].

United States Government's Response

In response to the SolarWinds cyberattack, the United States government launched an in-depth investigation and ultimately attributed the attack to Russia [21]. This attribution process involved extensive cooperation between U.S. intelligence agencies and cybersecurity firms, analyzing digital trails left behind by the hackers. The evidence led U.S. officials to conclude that the attack was likely conducted by APT29, also known as Cozy Bear, a group with connections to Russian intelligence.

Following this determination, the United States took decisive actions against Russia, aiming to address the immediate threat and deter future cyber aggression. One momentous response involved sanctions on Russian individuals and entities directly associated with the cyber operation, including members of Russian intelligence services [45]. Sanctions, as a common tool in U.S. foreign policy serve to economically isolate and penalize individuals and groups seen as security threats impacting their ability to engage internationally. These sanctions targeted both private entities and government-linked groups involved in the operation, effectively signalling U.S. disapproval and opposition to state-sponsored cyber activities.

In addition to sanctions, the expulsion of 10 Russian diplomats signified an intensification in diplomatic tensions. These diplomats identified as either directly or indirectly involved in espionage activities were removed from the United States, effectively reducing Russia's capacity to carry out intelligence operations on U.S. soil [45]. This expulsion underscored the United States' firm stance against what it viewed as a national security threat further straining relations between the two nations.

Beyond immediate punitive measures, the United States strengthened its cybersecurity defenses by adopting new security protocols and enhancing collaboration across both public and private sectors. This strategic redirection involved increased funding for cybersecurity, the establishment of more

comprehensive monitoring of supply chains, and heightened standards for vendors supplying software to government entities.

The U.S. response to the SolarWinds attack projects the realism theory in international relations which emphasizes state sovereignty, national security, and the pursuit of power to maintain stability and deter threats. Realism posits that the international system is anarchic, with each state primarily looking out for its own survival and interests. The United States, perceiving the attack as a direct threat to its security and sovereignty, responded with measures aimed at safeguarding its national interests. Sanctions and expulsions were enacted to deter future attacks and signal to Russia that any actions compromising U.S. security would have consequences. Realist theory holds that power is central in international relations. The imposition of sanctions and the expulsion of diplomats demonstrates how the United States exercised its economic and diplomatic power to discourage Russian cyber activities. This approach follows realism's emphasis on deterrence, indicating a strong response to prevent adversaries from engaging in further hostile acts.

In an anarchic international system, states cannot rely on others for security making self-help essential. The U.S. response involved bolstering its own cybersecurity defenses as a means of self-reliance, reinforcing its resilience against future attacks without relying on international mechanisms. Realism suggests that states act primarily in their own interests. The U.S. response focused on protecting its sensitive information, institutions, and infrastructure.

The Nature and Impact of Cyberwarfare on Arms Control

Cyberwarfare refers to the use of computer technology to disrupt or destroy the systems and networks of an adversary [10] Cyber-attacks include; hacking, malware attacks, phishing attack, social engineering, network infiltration, supply chains, and distributed denial-of-service (DDoS) attacks, pose a growing threat to sensitive information, critical infrastructure, and military operations. [6] specifies the threat of cyberwarfare which are;

- The global connectivity has led to the spread of production across many companies and states, increasing the possibilities of cyber warfare as vulnerabilities can be exploited in computers and routers.
- Trap doors, vulnerabilities built into computer programs, allow programmers to change the way the program works more easily and allow unauthorized personnel to gain full access.
- Logical bombs can be placed unnoticed on computers, it can erase entire computers or force electric grids to overload. Hackers can also gain access to other systems, such as a U.S government experiment, causing critical systems to go offline

Aspect	Description
Purpose	To disrupt or destroy competitor's digital capabilities or to protect one's digital capabilities. To gather intelligence on an adversary's cyber capabilities and intention

Strategy	Network exploitation, data infiltration, malware, denial of service attacks etc.
Targets	Government agencies, military, critical infrastructure etc.
Space	Cyberspace, including the internet
Preparation	Personnel, technology and training
Cost	Expensive; billions of dollars are used to develop and maintain cyberwarfare capabilities
Attribution	May be hard to find out due to the use of anonymity tools
Rules of Engagement	Not well defined
Impression	Fear of the unknown, and fear among the population
Damage	Economic and national security losses
Deterrence	Limited currently

Table 2; The nature of cyberwarfare

Source; [26], NATO, 2019 [5] ,[10]

[8] asserted that arms control is not about total elimination, but about monitoring the number, the production, the development, the storage of weapons or the deployment of troops. According to [39] Arms control is a strategic stability pillar, aimed to enhance security and prevent global nuclear annihilation. Its primary objectives include; reducing nuclear war risk, maintaining force equilibrium, reducing arms race costs, and limiting damage in case of war. These regulations may prohibit the use of specific types and qualities of weapons e.g, the Ottawa Convention, limit the testing of specific weapons; the Partial Nuclear Testing Prohibition Treaty prohibit the production and stockpiling of specific weapons.

As cyber warfare evolves, new strategies and approaches are needed to prevent and respond to such attacks Despite these threats, international arms control agreements have not fully addressed cyber warfare, focusing primarily on traditional weapons like nuclear, chemical, and biological weapons. However, traditional arms control regimes are inapplicable to cyberspace for reasons:

- Cyber warfare is still in its early development phase, making it nearly impossible to ban or restrict weapons.
- It is difficult to measure the relative strength of states in cyberspace;
- The tools used in the cyberspace are used for legitimate purpose e.g. penetration testing tools are used for securing network and conducting cyber attacks
- Cyberwarfare in cyberspace involves the accumulation of offensive and defensive capabilities, as there is no tangible, controllable objects like conventional forces or kinetic weapons making it hard to be detected
- Arms control focus on weapons and military capabilities, with cyberweapons ranging from benign to damaging systems, affecting systems from outside to inside.
- The challenges of monitoring compliance; and difficulties with enforcement; Arms control and disarmament agreements typically include provisions for verification, compliance, enforcement,

sanctions, confidence-building, dispute settlement, and cooperation for peaceful purposes, among other aspects.

- State and non-states actors like private entities can carry out offensive cyber operations, including those of armed forces and individuals. International agreements may require states to establish criminal law norms and exercise controls, but these are outside arms control logic.

[13] , [18], Maurer, 2018;[37], [8].

The Implications of the SolarWinds Hack on Global Security and International Arms Control

Absence of attribution

The SolarWinds hack exemplifies the complexities inherent in modern cyber warfare, particularly the challenge of attributing cyber-attacks to specific actors. In this instance, the attack which targeted numerous U.S. government agencies and private sector companies, underscores the difficulties in identifying the sources of cyber threats. This lack of attribution complicates accountability and diminishes the likelihood of effective consequences for those responsible. Cyber warfare, when launched on a global scale, poses significant threats to intelligence operations. The absence of tangible evidence, combined with attackers' capabilities to alter digital forensic clues, as noted by [26] creates an environment where discerning the authenticity of information becomes increasingly challenging. This uncertainty raises the risk of espionage, as it becomes difficult to ascertain the origins and validity of compromised materials.

Moreover, the SolarWinds hack exemplifies a broader concern regarding the interception and alteration of sensitive information across international borders. The implications of such actions are far reaching for global security and international arms control. In an era where state actors and non-state actors can exploit cyber vulnerabilities, the absence of clear attribution may lead to an erosion of trust among nations, potentially undermining diplomatic efforts and international agreements aimed at arms control.

Distrust among nations

The SolarWinds hack has further exacerbated existing distrust among nations, elucidating how cyber capabilities are increasingly employed for espionage purposes. State actors utilize these capabilities to steal sensitive information, trade secrets, and military plans from their adversaries. The public revelation of state-sponsored cyber espionage activities, particularly those attributed to nations such as China and Russia have strained diplomatic relations and further eroded trust among states [5]. This growing mistrust is also impacting international interactions, fostering skepticism about agreements, treaties, and diplomatic assurances [26]. In the context of the SolarWinds hack, the breach not only exposed vulnerabilities in U.S. cybersecurity but also amplified concerns about the integrity of international cooperation. Cyber operations challenge traditional diplomatic norms, creating barriers to collaborative efforts on pressing global issues, including arms control. As states grapple with the implications of the SolarWinds breach, the erosion of trust complicates the already delicate landscape of international arms control. The uncertainty surrounding the motivations and actions of other states leads to a defensive

posture, where nations may prioritize national security over cooperative measures. This environment of suspicion may ultimately hinder progress on vital agreements aimed at preventing arms proliferation and fostering stability.

No Clear rules of Engagement

The SolarWinds hack validates the pressing issue of the absence of clear rules of engagement in cyberspace, which creates ambiguity for states and non-state actors alike. In the current domain, the lack of established norms leaves nations to interpret and respond to cyber-attacks based on their own judgment and strategic interests. This ambiguity can lead to disproportionate responses, escalation of conflicts, and an increase in tensions between states. While there are ongoing efforts to establish responsible conduct in cyberspace, significant obstacles remain. Many states prioritize strategic competition over collaboration, which diminishes the willingness to engage in meaningful negotiations for arms control in this domain [27]. The ramifications of the SolarWinds breach illustrate how the absence of clear guidelines can escalate hostilities, as nations grapple with the implications of cyber espionage and the potential for retaliatory actions. Furthermore, the lack of clarity regarding acceptable behavior in cyberspace complicates the prospects for effective arms control agreements. Without agreed-upon standards, nations may hesitate to trust one another, fearing that any concession could be exploited by adversaries. This environment of uncertainty undermines the foundations of diplomacy, making it increasingly difficult to achieve consensus on crucial issues related to security and arms control.

Economic Impacts

The economic repercussions of the SolarWinds hack are gargantuan and far-reaching. According to [43] the estimated insured loss from the breach is approximately $90 million. This incident illustrates the risks associated with economic espionage, where trade secrets, innovation, and intellectual property are compromised. Such losses can severely impact national economies and industries, as the theft of critical information can lead to a decline in economic vitality and diminish the competitive advantage of affected sectors. When nations experience significant economic damage from cyber incidents, it can strain diplomatic relations and create an environment of mistrust, complicating efforts to engage in international arms control negotiations. The economic fallout from such attacks underscores the need for nations to bolster their cybersecurity measures to protect their assets and maintain a competitive edge in the global market.

Attack on Critical Infrastructures

The SolarWinds hack also shows the vulnerabilities of critical infrastructure, as it impacted various government agencies and private companies. Cyberwarfare poses a substantial threat to essential services, including power grids, water supplies, and communication networks, all of which are vital to public safety and national security. As noted by Saaida (2023), the risks associated with attacks on these infrastructures emphasize the urgent need for robust cybersecurity measures. The implications of such vulnerabilities extend beyond immediate economic damage; they can also destabilize national security and international

relations. When a nation's critical infrastructure is compromised, it may lead to heightened tensions and calls for retribution, further complicating diplomatic efforts and arms control discussions. The threat posed to critical infrastructure by cyber incidents like the SolarWinds hack necessitates a reevaluation of current security frameworks and international agreements regarding cyber operations.

Threats to National Security

The SolarWinds hack underlines some of the real, deep threats which cyber warfare poses to national security. Indeed, once having compromised access to important military and intelligence information, state-sponsored cyber actors might find themselves in a good position to grossly compromise the security of the nation targeted. Consequently, breaching into government agencies, military units, and intelligence services opens their avenue to gain confidential materials, military strategies, and vital intelligence information. This breach not only undermines the security and sovereignty of the affected countries but also has far-reaching implications for international relations [10]. According to realist theory, which emphasizes the anarchic nature of the international system and the prioritization of state power and security, the exposure of sensitive military and intelligence data can lead to a loss of strategic advantage and increased vulnerability to adversarial actions. In this context, states may respond to such breaches with heightened military preparedness or counter-cyber operations, further exacerbating tensions. Moreover, the risks associated with cyber intrusions extend beyond immediate national security concerns; they can also catalyze an arms race in cyberspace. Realist theory posits that nations operate under a self-help system, prompting them to enhance their cyber capabilities in response to perceived threats. This escalation can strain international relations and hinder cooperative efforts aimed at establishing norms and agreements for cyber conduct.

International Rivalries

As shown by the of case of SolarWinds hack, state-sponsored cyberattacks have the potential to intensify geopolitical tensions and destabilize international relations. Cyber warfare used for geopolitical objectives have the potential to worsen relations and spark diplomatic crises. The relations of the United States and Russia was strained which led to tension as Russia was blamed for the attack which has had significant adverse consequences for other states, including the USA and the United Kingdom [17], [7].

The Increased threat of Cyber warfare

The SolarWinds hack is a representation of the increased threat of cyberwarfare in the global setting [50] It has exposed the critical need to curb the rise of cyber warfare and the need for new arms control treaties to curtail its emergence. It is no longer a secret that the US, Russia, China, Israel, and North Korea are engaged in a severe, discrete and possibly explosive cyber warfare. A recent global survey found that the United States was the most feared potential attacker in cyberspace; China was second [42].

Conclusion and Recommendations

The SolarWinds hack of 2020 serves as a pivotal case study in understanding the complex relationship between cyber warfare and arms control. As this incident highlights, the integration of cyber capabilities into state strategies introduces new dimensions to national security threats, challenging traditional notions of warfare and deterrence. The implications of the hack extend far beyond immediate economic losses and breaches of sensitive information; they fundamentally reshape the dynamics of international relations. The lack of clear rules of engagement in cyberspace exacerbates mistrust among nations, undermining efforts to establish cooperative frameworks for arms control. As countries navigate the uncertain terrain of cyber operations, the realist perspective emphasizes the need for states to prioritize their security interests, potentially leading to an arms race in cyber capabilities. The erosion of trust caused by incidents like the SolarWinds hack calls for urgent dialogue and collaboration among nations to establish norms and agreements governing cyber conduct. It must be noted that the rise of cyber warfare challenges existing arms control treaties that primarily focus on conventional and nuclear weapons. As states increasingly rely on cyber capabilities for offensive and defensive operations, traditional arms control frameworks may become inadequate in addressing these evolving threats. Policymakers must consider how to integrate cybersecurity into existing arms control discussions, ensuring that treaties account for the realities of modern warfare. The following are recommended based on the findings of this study.

- Nations should work collaboratively to develop clear rules of engagement and norms governing state behavior in cyberspace, promoting accountability and reducing the likelihood of escalation.
- Governments and organizations must invest in robust cybersecurity infrastructure to protect critical systems from cyber intrusions and mitigate the impact of potential breaches.
- Ongoing diplomatic engagement is necessary to build trust among nations, facilitating discussions on cyber threats and arms control that can lead to more effective cooperative strategies.
- Collaborative initiatives, such as joint cybersecurity exercises and information-sharing platforms, can strengthen collective defenses against cyber threats and enhance global security.

References

[1] Alfonso, A.C & Forsyte Z (2022, December 8). Today in history: Reagan and Gorbachev sign the INF treaty. Wilson Centre. www.wilsoncentre.org Retrieved May 12, 2024

[2] Amosun, D (2022). Using Thematic Analysis and Threat Modelling to Analyse SolarWinds Attack. https://www.researchgate.net/publication Accessed May 20, 2024

[3] Azubuike, (2023) Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attack *Nnamdi Azikiwe Journal of Political Science (NAJOPS), Vol. 8(3)* 101-114

[4] Bronk, C. (2010) Toward Cyber Arms Control with Russia. *World Politics* https://www.worldpoliticsreview.com/toward Accessed May 15, 2024

[5] Cadioli, G (2023) The evolution of cyber conflicts and its impact on international security: a comprehensive analysis. *Universita' Degli Studi Di Padova Scuola di Economia e Scienze politiche European and Global Studies*

[6] Clarke, R. A. & Knake, R. K. (2010) *Cyber war: The next threat to national security and what to do about it,* New York: HarperCollins Publishers

[7] Coco, A, Dias, T & Benthem, T (2022) Illegal: The SolarWinds Hack under International Law

[8] Dahinde, M (2022) *How can arms control and disarmament contribute to a secure cyberspace?* Geneva: ICT4Peace Publishing www.ict4peace.org. Accessed May 15, 2024

[9] Den Dekker, G. (2004). The Effectiveness of International Supervision in Arms Control Law. *Journal of Conflict and Security Law, 9 (3),* 315-330.

[10] Digmelashvili, T (2023). The Impact of Cyberwarfare on the National Security. *Future Human Image, 19* 12-19

[11] Dittrich, P.J & Boening B (2017) More security in cyber space: The case for arms control. *Arbeitspapiere*. https://www.baks.bund.de/en . Accessed May 15, 2024

[12] Gorman, M. (2014) *Cybersecurirty: a guide to the fundamentals of cybersecurity.* Apress

[13] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. California Law Review, 100(4), 817-885.

[14] Hunker, J (2013). Cybersecurirty for critical infrastructure: a review of the literarture. *Journal of Information Systems Security, 12(2)* 1.14

[15] Hussaini, A., Qian, C., Liao, W., and W. Yu, (2022) "A taxonomy of security and defense mechanisms in digital twins-based cyber-physical systems," in 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics).

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

[17] Jibilian, I & Canales, K (2021, April 15). The US is readying sanctions against Russia over the solarwinds attack. Here's a simple explaination of how the massive hack happened and why it's such a big deal. *Business Insider*. www.business.com Accessed May 19, 2024

[18] Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, 38(2), 7-40.
[19] Knake, R (2021, March) "Why the SolarWinds Hack Is a Wake-Up Call," *Council on Foreign Relations*. https://www.cfr.org/article Accessed May 18, 2024
[20] Lee, J (1999). Arms control and disarmament. www.publications.gc.ca/Pilot. Retrieved May 13, 2024
[21] Lemon, J. (2020). SolarWinds Hides List of Its High-Profile Corporate Clients After Hack. *Newsweek*. https://www.newsweek.com. Accessed May 18, 2024
[22] Li Y & Liu, Q (2021) "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments*," Energy Reports, 7.* 8176–8186
[23] Malwarebyteslabs. (2021). SolarWinds advanced cyberattack: What happened and what to do now https://blog.malwarebytes.com/threat-analysis Accessed May 18, 2024
[24] Marelli, M. (2022). The SolarWinds hack: lessons for international humanitarian organizations. International Review of the Red Cross 104 (919), 1267–1284.
[25] Maybaum, M & Tölle, J (2016) Arms Control in Cyberspace – Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods
[26] Meyer P (2011) Cyber-security through arms control, *The RUSI Journal, 156(2)* 22-27
[27] Miller, S. (2022). Hard Times for Arms Control What Can Be Done?. The Hague Centre for Strategic Studies. www.hcss.nl. Retrieved May 13, 2024
[28] Morgenthau, H. J. (2006). Politics Among Nations: The Struggle for Power and Peace. McGraw-Hill.
[29] Munro, A. (2024, March 30). nuclear proliferation. Encyclopedia Britannica. https://www.britannica.com/topic/nuclear-proliferation. Retrieved May 13, 2024
[30] Nakashima, E and Timberg C, (December 2020). "Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce," *The Washington Post*. https://www.washington.org. Accessed May 15, 2024
[31] Nye Jr, J.S (2015 October 1) Opinion; The world needs new norms on cyberwarfare. *The Washington Post*. https://www.washingtonpost.com/opinions/the-world-Accessed May 15, 2024
[32] Nye, J.S (2019, October3). Can cyberwarfare be regulated? Austrialia Strategic Policy Institute.www.aspistrategist.co
[33] Oladimeji, S & Kerner, S.M (2023, November 3). SolarWinds hack explained:everything you need to know. *TechTarget. www.techtarget.com*. Accessed May 20, 2024
[34] Perlo-Freeman, S. (2024, April 19). arms race. Encyclopedia Britannica. https://www.britannica.com/topic/arms-race Retrieved May 13, 2024
[35] Rabkin, A. (2015, March 3). Cyber-arms cannot be controlled by treaties. AEI. www.aei.org Accessed May 20, 2024
[36] Reinhold, T., Reuter, C. (2019). Arms Control and its Applicability to Cyberspace. In: Reuter, C. (eds) Information Technology for Peace and Security. Springer Vieweg, Wiesbaden.

[37] Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4-37.

[38] Sanger, D. E., N. Perlroth E. Schmitt. (2020, December 14). "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit." New York Times, https://www.nytimes.com Accessed May 19, 2024

[39] Schelling, T. C. and Halperin, M. H., (1961). *Strategy and Arms Control*. New York: Twentieth Century Fund

[40] Schneider, B.R (2024, May 8). Chemical weapons convention. Encyclopedia Britannica. www.britannica.com/topic/chemical-weapons-convention. Retrieved May 12, 2024

[41] Senate RPC (2021, January 29). The SolarWinds cyberattack. Senate RPC. www.senate.gov Accessed May 18, 2024

[42] Sexton, J (2010, January 30) "U.S. Most Likely Suspect in Cyber Wars: IT Survey," China. https://www.china.org.cn Accessed May 20, 2024

[43] Shah, S (2021, January 12). The financial impact of SolarWinds breach. *Bitsight.* www.bitsight.com Accessed May 18, 2024

[44] Schmitt M N (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press

[45] Teh, (2021, April 15). US set to sanction on Russia individuals, 24 entities for influencing the 2020 election. Business Insider. www.africa.businessinside.com Accessed May 20, 2024

[46] Thompson, K,W (2024, February 5). Arms Control. Encyclopedia Britannica. www.britannica.com/topic/arms-control. Retrieved May 12, 2024

[47] Tran, C (2021). The SolarWinds Attack and Its Lessons. The SolarWinds Attack and Its Lessons https://www.e-ir.info/2021/06/17/the-solarwinds-attack-and-its-lessons Accessed May 15, 2024

[48] Trezza, C (2017). Cyber security: a new chapter for arms control. *NATO.* www.natofoundation.org. Accessed May 19, 2024

[49] Turton W & Mehrota, K (2020, December 15) "FireEye Discovered SolarWinds Breach while Probing Own Hack", Bloomberg.www.bloomberg.com Accessed May 18, 2024

[50] Valeriano, B., Jensen, B. M & Maness, R.C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion.* New York: Oxford University Press.

[51] Waltz, K. N. (1979). Theory of International Politics. Addison-Wesley.

[52] Wheeler. T (2021. March 4). The danger in calling the solarwinds breach an act of war. Broojings. www.brookings.edu Accessed May 18, 2024