p-ISSN : 2708-2121 | e-ISSN : 2708-3616

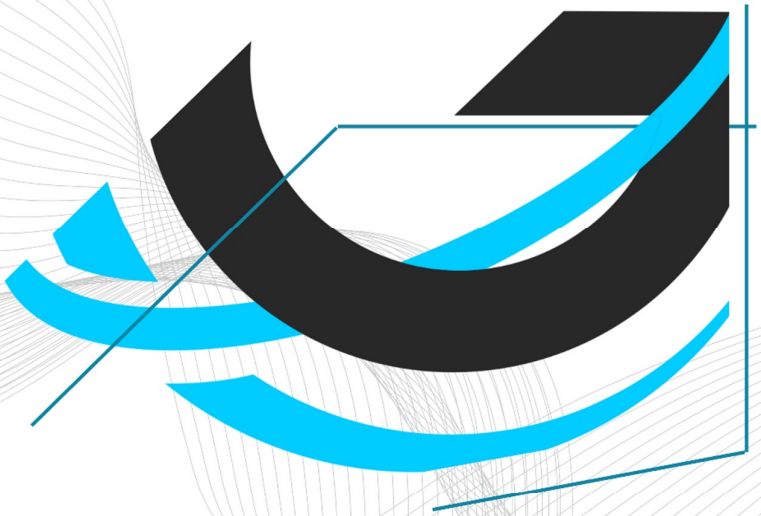
DOI(Journal): 10.31703/gsssr
DOI(Volume): 10.31703/gsssr/.2024(IX)
DOI(Issue): 10.31703/gsssr.2024(IX.I)

www.gsssrjournal.com

Global Strategic and Security Studies Review
surveilling humanity

GSSSR

GLOBAL STRATEGIC & SECURITY STUDIES REVIEW



VOL. IX, ISSUE I, WINTER (MARCH-2024)

HumanityPublications
sharing research
www.humapub.com
US | UK | Pakistan

Double-blind Peer-review Research Journal
www.gsssrjournal.com

Humanity Publications(HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Article Title

Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran

Global Strategic & Security Studies Review

p-ISSN: 2708-2121**e-ISSN:** 2708-3616

DOI(journal): 10.31703/gsssr

Volume: IX (2024)

DOI (volume): 10.31703/gsssr.2024(IX)

Issue: I (Winter-March 2024)

DOI(Issue): 10.31703/gsssr.2024(IX-I)

Home Page
www.gsssrjournal.com

Volume: IX (2024)
https://www.gsssrjournal.com/Current-issues

Issue: I-Winter (March-2024)
https://www.gsssrjournal.com/Current-issues/9/1/20234

Scope
https://www.gsssrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gsssr/submissions

Google Scholar

Visit Us

Abstract

The escalating prominence of cyber security issues worldwide has intensified concerns about cyber warfare within the context of the strained relationships among the United States, Israel, and Iran. The hypothesis posits that cyber warfare is inevitable and could lead to catastrophic consequences. Using qualitative research methods from secondary sources like books, journals, etc., this study aims to elucidate the nature of these threats. The research delves into research questions i.e. What are the fundamental cyber warfare strategies employed by the United States, Israel, and Iran, and how they contribute to the escalating tensions among them? How do cyber threats originating from the USA and Israel impact Iran's national security? What are the possible future outcomes of cyber warfare between these nations? Despite limitations such as observational and descriptive study constraints, thematic focus on the security dynamics between these nations, this research contributes to understanding the evolving landscape of cyber security.

Keywords: Cyber Warfare, Peace, Stability, Cyber-attacks, Strategic Weapon, Capabilities, US Foreign Policy, Counter Measures

Authors:

Urwa Sajjad Ahmed Abbasi: (Corresponding Author)
Mphil Scholar, School of Politics and International Relation, Quaid-i-Azam University, Islamabad, Pakistan.
(Email: Urwa.sajjad1999@gmail.com)

Pages: 44-56

DOI: 10.31703/gsssr.2024(IX-I).04

DOI link: https://dx.doi.org/10.31703/gsssr.2024(IX-I).04

Article link: http://www.gsssrjournal.com/article/A-b-c

Full-text Link: https://gsssrjournal.com/fulltext/

Pdf link: https://www.gsssrjournal.com/jadmin/Auther/31rvIolA2.pdf

Humanity Publications (HumaPub)
www.humapub.com
Doi:https://dx.doi.org/10.31703

Citing this Article

04		Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran						
		Author	Urwa Sajjad Ahmed Abbasi		DOI	10.31703/gsssr.2024(IX-I).04		
Pages		44-56	Year	2024	Volume	IX	Issue	I
Referencing & Citing Styles	APA	Abbasi, U. S. A. (2024). Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran. *Global Strategic & Security Studies Review*, *IX*(I), 44-56. https://doi.org/10.31703/gsssr.2024(IX-I).04						
	CHICAGO	Abbasi, Urwa Sajjad Ahmed. 2024. "Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran." *Global Strategic & Security Studies Review* IX (I):44-56. doi: 10.31703/gsssr.2024(IX-I).04.						
	HARVARD	ABBASI, U. S. A. 2024. Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran. *Global Strategic & Security Studies Review,* IX, 44-56.						
	MHRA	Abbasi, Urwa Sajjad Ahmed. 2024. 'Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran', *Global Strategic & Security Studies Review*, IX: 44-56.						
	MLA	Abbasi, Urwa Sajjad Ahmed. "Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran." *Global Strategic & Security Studies Review* IX.I (2024): 44-56. Print.						
	OXFORD	Abbasi, Urwa Sajjad Ahmed (2024), 'Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran', *Global Strategic & Security Studies Review,* IX (I), 44-56.						
	TURABIAN	Abbasi, Urwa Sajjad Ahmed. "Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran." *Global Strategic & Security Studies Review* IX, no. I (2024): 44-56. https://dx.doi.org/10.31703/gsssr.2024(IX-I).04.						

e-ISSN:2708-3616 Volume:IX (2024) Issue: I-Winter (March-2024) p-ISSN:2708-2121

Global Strategic & Security Studies Review
www.gsssrjournal.com
DOI: http://dx.doi.org/10.31703/gsssr

Pages:44-56 URL:https://doi.org/10.31703/gsssr.2024(IX-I).04 Doi: 10.31703/gsssr.2024(IX-I).04

Cite Us

Title

Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran

Contents

- Introduction
- Literature Review
- Theoretical Framework
- Cyber Security as a Threat to National Security
- US- Israel Cyber Strategy
- Iranian Cyber Strategy
- Recommendations
- Conclusion
- References

Abstract

The escalating prominence of cyber security issues worldwide has intensified concerns about cyber warfare within the context of the strained relationships among the United States, Israel, and Iran. The hypothesis posits that cyber warfare is inevitable and could lead to catastrophic consequences. Using qualitative research methods from secondary sources like books, journals, etc., this study aims to elucidate the nature of these threats. The research delves into research questions i.e. What are the fundamental cyber warfare strategies employed by the United States, Israel, and Iran, and how do they contribute to the escalating tensions among them? How do cyber threats originating from the USA and Israel impact Iran's national security? What are the possible future outcomes of cyber warfare between these nations? Despite limitations such as observational and descriptive study constraints, and thematic focus on the security dynamics between these nations, this research contributes to understanding the evolving landscape of cyber security.

Authors:

Urwa Sajjad Ahmed Abbasi: (Corresponding Author)
Mphil Scholar, School of Politics and International Relation, Quaid-i-Azam University, Islamabad, Pakistan.
(Email: Urwa.sajjad1999@gmail.com)

Keywords: Cyber Warfare, Peace, Stability, Cyber-attacks, Strategic weapon, Capabilities, US Foreign Policy, Counter Measures

Introduction

Since the turn of the century, the world has experienced a great number of shifts, many of which are best demonstrated by the expansion of science and technology. These changes have not only influenced the way we live our lives, but they have also given rise to new concerns regarding the state of global security. Let's take a look at cyber warfare, which is often referred to as a non-traditional threat to security. It is described as an attack on a nation's computer network or as a series of attacks using the internet as the principal tool to carry them out. Attacks on computer networks have the potential to bring down important computer systems, damage the economy, bring down civilian and government infrastructure, and inflict catastrophic damage on the state. The bulk of the time, nation-states will launch attacks on other countries as part of their

cyber warfare operations. On occasion, though, terrorist organizations and other non-state actors will also carry out attacks of this nature in an effort to achieve their objectives.

The primary objective of this paper is to provide an analysis of the tensions that exist between the United States of America, Israel, and Iran in the context of cyber warfare. Cyber warfare can be seen in the form of "The Stuxnet worm" (2010), "The Flame," "The Gauss Malware," Distributed Denial of Service (DDoS), and Ransomware attacks, which were used to attack the Iranian Nuclear Program through infected USBs to obtain data from the Natanz Enrichment plant The use of these cyber weapons raises the question of how successful they can be and under what circumstances they may be considered a genuine threat to Iran, the United States, and Israel. However,cyber-attacks are a new type of security danger that has emerged as a result of improvements in the realm of information technologies. These attacks have the potential to alter the predominant way in which conflicts are perceived by people. As a result of the fact that this danger is still in its beginning and is subject to ongoing development and modification, it is challenging to envision how it might emerge in the future or how it might be utilized in armed conflicts.

However, one must keep in mind that both the European Union and the North Atlantic Treaty Organization (NATO), in addition to the United States of America, have already recognized cyberspace as a new military domain. This research analyses how conflicts are evolving as a result of the growth of this new domain. These conflicts differ from traditional ones in both methods and means, and they are unaffected by the principles of international law that apply to armed conflicts and wars. Despite this, many authors cannot draw the conclusion that the risk posed by this new kind of conflict is any lower. Cyber-attacks, despite taking place in the virtual realm, can have significant real-world effects. This research uses a comparative analysis of various approaches to this topic before examining future developments in cyberwarfare, specifically whether it could eventually become its own branch of warfare or if it will only be used as an adjunct to conventional warfare, as it has since the emergence of "hybrid warfare." This research contributes to the resolution of cyberattack-related issues and will offer some counterstrategies from an Iranian perspective to address the cyber situation going forward. It also gives the states involved in the conflict a better understanding of how to handle specific potential challenges both now and in the future (Epps, 2013).

Literature Review

As mentioned in Katie Terrell, Hanna Kevin, and Ferguson's article titled "Cyber warfare," Cyberwarfare, as eloquently defined by Linda Rosencrance, is the employment of cyberattacks against a nation-state with the goal of causing it great harm, up to and including physical warfare, disruption of critical computer systems, and loss of life. The precise actions that are thought to be included in the definition of cyber warfare, however, remain a matter of debate among experts. There are some gaps in the literature, despite the Department of Defense's (DOD) assertion that using computers and the internet to wage war in cyberspace is a threat to national security. It is unclear why some actions are classified as warfare while others are merely classified as cybercrime, and it is also unclear how these actions are causing instability for states (Director et al., 2021).

Within the context of the paper titled "Cyber security: A National Security Issue? The author, Daniele HadiIrandoost (Irandoost, 2018) discusses cyber security for policymaking reasons and has debated the question that why cyber war is or is not inevitable. Both of these explanations can be found in the author's writing. The author continued by recommending the implementation of a method that was better-rounded, suggesting that it should be founded on concrete data and expert knowledge, which should be combined with analytical perspectives from the humanities. Finally, the author shows how various states may view what constitutes adequate cyber security differently because they face different kinds of cyber threats. All things considered, one topic that has to be addressed right now, especially in liberal democracies, is how to assign different responsibilities to public and private entities in order to guarantee cyber security. According to the author, information sharing and collaborative efforts between the public and private sectors are necessary to counteract the use of cyber warfare. He concluded by saying that we must have a thorough awareness of both the technological and technical facets of cyber security. The many

cyberattacks that have occurred in the past, including those against Iran, Israel, and the United States of America, lend credence to this claim. Because of this, cyber security is a crucial component of national security that necessitates a thorough understanding. (Jr. & Arnold, 2023)

The information presented in the Al Jazeera story titled "US Imposes New Sanctions on Iran over Albanian Cyber-attack," (Staff, 2022) Staff says while the two nations US and Iran battle to find a way back into the 2015 nuclear deal, the Biden administration has placed further fines on Iran's Ministry of Intelligence and Security for what it dubbed "malign cyber conduct." According to the US Treasury Department, the penalties were imposed as punishment for a cyber-attack that occurred in July and caused damage to websites belonging to the Albanian government. Washington and Tirana both pointed the finger of blame at Tehran for the incident. Penalties were placed on Iranian intelligence minister Esmail Khatib one day after Washington imposed sanctions on various Iranian firms, accusing them of being complicit in the creation and transfer of drones to Russia for use in the conflict in Ukraine.

The United States of America is committed to effectively enforcing its sanctions against both Russia and Iran, as well as to holding Iran and those who support Russia's offensive war against Ukraine accountable for their actions. As a direct result of the sanctions, the targeted individuals and businesses will have their assets frozen in the United States, and it will be illegal for citizens of the United States to engage in commerce with the sanctioned parties. According to the United States Department of State, which is in charge of the indirect nuclear discussions with Iran, the paper claims that Washington would use any and all appropriate instruments to defend against cyber-attacks directed against the United States and its allies. There are certain gaps in the literature as the author is unable to illustrate how cyber warfare is affecting the security of Iran (Al Jazeera, 2024).

Israel launched a missile attack against Hamas in May of this year after the Israeli Defense Force claimed that the group's hackers were targeting Israeli targets. Under international law, the United States would have the right to carry out a preemptive physical strike toward Iranian targets if they had reason to think that Iran was preparing to launch a cyberattack against critical infrastructure. However since a significant cyberattack might be planned ahead of time or executed swiftly, it is challenging to predict when one will start. This makes it tough to protect against. The article basically explains how cyber threats are affecting the security of Iran but there are still some gaps in the literature the unable to highlight any countermeasures states need to opt to prevent cyber-attacks. Secondly, the author had not elaborated on how the world is going to be suffering from these cyber attacks (Imperva, 2023b)

In the piece titled "Invisible US - Iran Cyber War," written by Andrew Hanna, (Hanna, 2023) the author elaborates on the tensions that are increasingly being played out in invisible cyberspace between the United States of America, Israel, and Iran. Both governments admitted that launching cyber-attacks was a primary focus of their respective tactics. It was unclear how widespread the problem was, but it appeared that the internet had become a battleground. Cyber offered a substitute for kinetic military action, which had the potential to escalate into full-scale conflict and was something that states wanted to avoid. According to the author, Iran has identified the perpetrators of the attacks, as well as the organizations that supported and assisted the crimes, and in certain instances, the state that sponsored the attacks. Given Mr. Trump's directive, it is quite logical to presume that the United States government and Israel will be the primary suspects in any future cyber-attacks against Iran. This is the case unless it can be demonstrated that the assaults were carried out by another party. Reports indicate that in September of 2018, President Trump handed the Central Intelligence Agency (CIA) an expanded ability to execute cyber-attacks against infrastructure that is used by the general people.

Theoretical Framework

Realism, a dominant theory in international relations, provides a useful lens for understanding the role of cyber tools as a threat to peace and stability. It focuses on the power dynamics between sovereign states, emphasizing the pursuit of national interest, security, and survival in an anarchic international system where no central authority exists above states. The primary concern of states is to ensure their survival and sovereignty,

and controlling and protecting their territory, including cyberspace, is crucial for national security. Cyber tools and cyber terrorism pose significant threats to these core interests by potentially undermining a state's sovereignty and stability. Realists emphasize military power and the right of states to defend themselves; thus, cyber-attacks targeting critical infrastructure can be equated to acts of war, justifying self-defense. In an anarchic international system, states must rely on their capabilities to ensure security, as exemplified by ongoing cyber conflicts between states like the US, Iran, and Israel. These engagements reflect geopolitical competition, where cyber actions are driven by the desire to assert dominance, counter rivals, and protect strategic interests. The unique characteristics of cyberspace, such as anonymity and difficulty in attribution, challenge deterrence, potentially leading to unchecked cyber aggression and escalation into broader conflicts. While international laws and norms exist, realists view them as secondary to the interests of powerful states, as demonstrated by the disregard for cyber norms by the US and Iran (Antunes, 2018).

Additionally, realism highlights the importance of forming alliances to balance threats, reflected in the US's cyber strategy of deepening alliances and forming partnerships to enhance collective cyber defense capabilities. Within this realist framework, the interactions in cyberspace are seen as extensions of traditional power struggles, where states use cyber capabilities to achieve strategic objectives. The geopolitical dynamics between the US, Iran, and Israel illustrate how cyber tools are integrated into broader security strategies, with each state leveraging cyber operations to gain advantages, disrupt adversaries, and safeguard national interests. Realists argue that in the absence of a central authority, states must continuously enhance their cyber capabilities to defend against potential threats, reinforcing the anarchic nature of the international system. The complexity of attribution in cyberspace also introduces challenges in establishing clear deterrence, leading to a security dilemma where states may engage in preemptive or retaliatory cyber actions to maintain their security posture. This contributes to a cycle of cyber escalation, reflecting the realist view that international relations are inherently conflictual and competitive. Moreover, the realist perspective acknowledges that while international norms and agreements on cyber conduct exist, they are often undermined by the strategic imperatives of states, as seen in the persistent cyber confrontations and the prioritization of national security over adherence to international frameworks. Finally, the formation of strategic alliances and partnerships in cyberspace is a critical component of a realist strategy, enabling states to pool resources, share intelligence, and strengthen their collective cyber defense mechanisms, thus enhancing their ability to navigate the complexities and threats of the cyber domain (Craig & Valeriano, 2018).

Cyber Warfare "A Perfect Strategic Weapon"

In the course of the last few years, the terms "cyber-attacks" and "cyber warfare" have emerged as two of the most prevalent ones in discussions regarding the nature of future conflicts and the formulation of innovative strategies for ensuring safety. However when it comes to military and security plans, decision-makers in the majority of nations defining contemporary international affairs are increasingly focusing on "cyber." States have been investing mainly in offensive cyber capabilities and creating military cyber units since about twenty years ago, seeing cyberspace as the "next big thing in security." Regardless, states now recognize cyberspace as the "next big thing in security." On the contrary, the majority of the conversation in the academic literature has focused on the effectiveness of cyberattacks and whether or not they pose a significant threat as a completely new form of warfare (Imperva, 2023).

Only a few authors have attempted to characterize the nature of cyberattacks thus far, and there is no consensus as to what these attacks will look like going forward. From a historical perspective, every new development in technology gave rise to fresh concepts that became essential to those who thought about national security. Following the terms "air power," "nuclear and thermonuclear weapons," and "space as a potential conflict area," the term "cyber" has become the newest buzzword in the security literature industry. The early Internet pioneers saw only the benefits of networking and simpler data exchange when they created the global network that gave rise to cyberspace. However, cyber also brought with it a

plethora of new security risks and challenges, one of which being the possibility of interstate conflict in the cyber realm. It is generally agreed upon that cyberattacks pose a serious risk to national security. Because they make it possible to wage war in new ways, they are frequently referred to as a state's "ideal strategic weapon" (Li & Liu, 2021).

Panic and intimidation: When used in conjunction with other kinetic, or conventional, weapons, the employment of cyber weapons, which have been described as "the perfect strategic weapon," is both significantly more noticeable and successful. In these situations, the main goal of cyberattacks is to partially or completely disable defense systems, including conventional and cyber defense. This is achieved by disseminating propaganda through attacks of various kinds, such as those on media and institutional websites, numerous applications, cellphones, personal IDs, and so forth, and intimidating civilian populations by destroying or deactivating vital civilian infrastructure, among other things. This results in panic and illogical behavior on the part of the populace. In this context, for example, in 2010 the United States and Israel launched the Stuxnet cyberattack against Iran. This attack was designed to disable the Iranian Nuclear Program by using an infected universal serial bus for the purpose of data collecting. In this particular instance, cyberspace proved to be an effective tactical weapon for the parties engaged in the fight. Because of the ongoing battle, neither government felt the need to disguise its actions, therefore the use of itself was a very painless process. This indicates that hybrid wars will, in any event, virtually probably continue to be the vehicle through which cyber warfare will manifest itself (Dykstra et al., 2020).

Deterrence: In this regard, new trends in signaling and deterrence have emerged recently, with state representatives emphasizing the development of cyber defense capabilities over the announcement of particular cyberweapons' development and potential repercussions. This is different from earlier trends, wherein states disclosed the creation of particular cyberweapons and the potential repercussions. "Deterrence will necessarily be based more on refusing any benefit to attackers than on demanding costs (for an attack) through retaliation," said William Lynn III, the deputy secretary of defense for the United States. On the other hand, adversaries may be deterred from conducting operations outside of the cybersphere by using cyberattacks. This phenomenon is exemplified by the 2010 Iranian uranium enrichment facility attack that was reportedly carried out by the Israelis and Americans using the "Stuxnet" worm. The attack essentially destroyed the facilities and sent a strong message to Iran telling it to stop this program. If these attacks are effective, they may send out a signal strong enough to deter some states from participating in specific activities (Fischer, 2019).

Iran places neither deterrence nor defense as its top priority. The majority of the time, cyber-attacks are carried out in order to exact revenge or as a form of coercion. Iran is not just concentrating its attention on its enemies in the West, such as the United States, but also on Middle Eastern regional targets, especially Saudi Arabia. Various types of attacks are conducted against these targets, irrespective of whether they are American, Saudi Arabian, or another type of target. An example of a normal cyberattack is the one that the Iranian hackers group conducted in 2019 against LinkedIn users connected to Middle Eastern government, banking, and energy companies. In 2019, an Iranian covert operations cell aimed at the digital networks of the Saudi government and the US administration and industry, which is a further common and typical example. Attacks that target multiple states are much less common. In 2012, Iran started attacking the U.S. and its allies with its "Shamoon virus." The malware was designed to target oil corporations in Saudi

The Use of Cyber Tools as a Threat to Peace and Stability

In a nutshell, cyberterrorism poses a risk to the peace and security of the world community. In a court of law, this constitutes a violation of the fundamental principles upheld by the United Nations. By virtue of their sovereign status, states have the authority to exercise control over the space-based infrastructure and activities that take place within their borders, as well as to shield their territories from illegal activity. Therefore, the legal procedures and principles of cyber-attacks must prevent the parties from employing force against the territorial integrity, political independence, or any other circumstance that is incompatible with

the goals and guiding principles of the United Nations (UN). As a consequence of this, the sovereign rights of all governments that are members of the United Nations, as well as the rights of subjects that are governed by international law and should be safeguarded, are equivalent. Some academics are of the opinion that assaults carried out by cyber-terrorists are similar to those carried out by armed terrorists and that this makes them an issue that relates to both self-defense and the long-term political interest of a country.

Cyberterrorism is a threat to this interest, which in turn affects the stability of countries all over the world. The national and international interests of many governments and non-state actors are concerned with global peace, security, and stability. Hence it is strongly suggested that an international legal instrument be specified, the signing of which is mandatory for all governments that are members of the United Nations as well as prominent non-state entities (United States Institute of Peace, 2015).

Deception and Disruption: Iran, the United States of America, and Israel have been involved in mutual offensive covert cyber-actions for quite some time, although neither country has publicly claimed responsibility for them. More than a decade ago, Iranian officials discovered the malware known as Stuxnet in the uranium enrichment centrifuges in one of Iran's nuclear facilities. This discovery marked the first public evidence of the use of cyber weapons against Iran, which is ultimately causing deception and disruption for Iran. The ongoing covert conflict has been given a new public dimension as a result of the reported intensification of cyber-attacks and incursions carried out by Iran, the United States, and Israel. These incidents have garnered attention and media from around the world. There was an attempt in April 2020 to breach Israel's water and sewage infrastructure. In May 2020, there was a cyber-attack on Iran's ShahidRajaee port. In July 2021, there were cyber-attacks on Iranian transportation systems. In October 2021, there was a hack of an Israeli hosting company and a leak of users' personal information. There was also a cyber-attack that disrupted gas stations across Iran in the same month. These are just some examples. (Baram, 2022)

Create Chaos and Distrust: One of Iran's first known instances of cyberwarfare in the last ten years was a spate of distributed denial of service (DDoS) attacks against the US financial sector between 2011 and 2013. The US National Security Agency understood these attacks, code-named Operation Ababil, as a reaction to Western attempts to stall Iran's nuclear program. Financial institutions in the United States were targeted by campaigns ascribed to the Izz ad-Din al-Qassam Cyber Fighters (QCF), a front organization affiliated with the Islamic Revolutionary Guard Corps. Massive computer networks known as "botnets" are used in DDoS

attacks to target targets, making it difficult to attribute the attack and ultimately leading to mistrust and confusion.

May Lead to Physical War: The United States of America and the Islamic Republic of Iran do not have inherently hostile foreign policies or cyber strategies; yet, the interactions that these two countries have had in the past in the realm of cyberspace demonstrate that peace can never be assured. Because of the way each country's foreign policy encourages competition with the other, one of the two countries will always want to "one-up" the other. To oppose Iran's influence in the region, the United States must keep its control over the Middle East, while Iran seeks to be acknowledged as a major world force. These two divergent agendas will always come into conflict with one another, which will lead to conflicts similar to those that have occurred in the past. The most significant conflict yet was Stuxnet; nevertheless, it is possible that future conflicts will be of a similar magnitude. When assessing what an actual or possible escalation would look like, there are a lot of factors that need to be taken into account. Despite the fact that battles that take place are generally restricted to the cyber domain, states have the capacity to take the fight outside of the cyber realm. As can be observed from the US and Iranian governments' respective foreign policies, the likelihood of this occurring is extremely low. Nevertheless, shifting dynamics and varying events might be a plausible justification for resorting to physical reprisal (Aminloo & Vitone, 2022).

For instance, the Israeli Defense Force launched an airstrike against a building they believed to have been housing the attack's infrastructure after

claiming that Hamas hackers were behind an attack on Israel. That being said, the consequences of a deliberate cyberattack could be far worse. According to the IPI Global Observatory, the US may be legally justified in taking preemptive military action against Iranian targets if it thought Iran was about to launch a cyberattack against vital infrastructure. (If the US believed that Iran was about to launch a cyberattack against critical infrastructure.) This statement is applicable to Iran as well. These violent assaults may have disastrous impacts in the future and may bring these two nations to the face of armed conflict (Aminloo & Vitone, 2022b).

Cyber Security as a Threat to National Security

Cybersecurity has a significant role to play in the broader field of security studies. To achieve this objective, an examination of the securitization process and the ways in which different stakeholders have shaped cyber risks must be done. This section aims to show that cyber threats can be considered national security threats and that security studies theories—more specifically, the Buzan vulnerabilities and threats framework—can therefore be applied to cyber security research and policy. In his landmark paper "National Security" as an Ambiguous Symbol, Arnold makes the case that political judgments, not technological or legal ones, are made regarding whether a threat to national security should be classified and what steps should be taken in response. This is due to the fact that it is a political choice to identify a threat as one to national security. Securitization occurs when a problem is portrayed as posing a serious danger (usually to the whole nation-state) to the extent that it necessitates emergency measures (the ones that go beyond routine political actions). Put another way, a problem is securitized when it is claimed that it necessitates emergency measures (i.e., actions beyond customary political ones) (Arnold, 1952).

As a result, in order to participate in the process, you are going to need a victim, a threat, and a knowledge of the threat that the victim faces. Criminals, hackers, terrorist organizations, and even nation-states themselves can all pose a risk in cyberspace. There is a wide variety of people who could end up being victims of these various threat vectors. To commit fraud that, in the interconnected world of cyberspace, would make all persons in a nation possible victims, the threat actors might be in the business of stealing people's identities and using them for fraudulent purposes. There is also the possibility that the threat actors are engaging in industrial espionage. In the instance of industrial espionage, the direct victims are the targeted businesses; however, if the knowledge that was taken was the blueprint for a new type of combat aircraft, the taxpayer may once more be deemed a victim (Arnold, 1952b).

When the state and its institutions are acknowledged as the victims, the existential threat could manifest as the current government being overthrown or as certain regions of the nation seceding from the national union. When a citizenry faces an existential threat to their well-being, either directly or indirectly due to the collapse of state institutions, public action may be justified on the grounds that national defense is a public good. When there is a direct threat to national defense, this argument can be made. Because they are tasked with representing the interests of their constituents, politicians are consequently forced to securitize risks to specific citizens. The ambiguous nature of national security in cyberspace also adds to the debate about the scope of national security in the academic field of security studies. Neorealists would likely argue against adding cyber security to the agenda of security studies as long as there is disagreement over the actual effects of cyberattacks on a country's military might and physical security. This is due to the neorealist viewpoint that it would be inefficient to advance the security studies agenda (Ministry of Foreign Affairs, 2022).

For instance, they acknowledge that challenges to security can originate from political and military actors, but they also underline the possibility of dangers to national security originating from economic, sociological, and ecological factors (Buzan, 1991). In addition, the referent object that is in danger might include any actor at any level, from the private to the public sphere, including businesses, countries, states, and local communities. In this way, even in cases where an actor is a person and an existential danger is the possibility of financial collapse, cyber threats would undoubtedly qualify as security concerns for a referent object. It is evident that nations have

decided there is a cyber-security element to national security, even though neo-realists and other security studies specialists would disagree on the role of cybersecurity in the field. As long as nation-state representatives continue to securitize cyber threats in speeches and plans, we must consider the role that these issues play in national security. For the US, the Middle East is a difficult and complicated region. The US considers it essential to keep a presence in the region in order to prevent future conflicts and stabilize it in a way that will protect the US itself. American strategists came to the conclusion following World War II that the US should concentrate on the Middle East in order to deter any hostile nation seeking to seize control of a region that possessed substantial geopolitical and material significance. The Middle East satisfies three requirements to be classified as a region of high geopolitical and material significance. First off, the region contains some of the largest oil reserves in the world. The Middle East is vital to US foreign policy goals due to two factors: oil production and energy availability.

The Persian Gulf countries hold about ten percent of the United States' total oil reserves. Iran is one of them, possessing the fourth-largest oil reserves globally and the second-largest oil reserves in the Middle East. Due to Iran's vast oil reserves, the US is under pressure to delay making snap decisions. The US intelligence community warned in 1982 that Iraq was dangerously close to collapse in the midst of the Iran–Iraq War, which lasted from 1980 to 1988. In order to prevent Iran from gaining control of the Persian Gulf and its vast oil reserves, the US assisted Iraq in its counteroffensive strategies. Furthermore, disputes arise around the Strait of Hormuz. Located in the Persian Gulf, specifically this strait, is one of the most significant bottlenecks for international commerce. The strait is primarily under Iranian control, but nations such as the US take measures to prevent Iran from militarizing it and jeopardizing global oil supplies. In order to stop Iran from escalating its military presence in the Strait of Hormuz, the United States of America must continue to be present in the Middle East and endure economic consequences (Hare, 2010b).

The US should continue to be present in the Middle East for a variety of geopolitical reasons. Many people believe that Iran is a country that fuels Middle East instability. The United States has been attempting to balance the Iranian risk by forming alliances with friendly Arab governments and giving Israel military support to bolster their defense ever since the Nixon Doctrine, which defined the "twin pillar policy" in the Middle East, during the Cold War. This is something that the USA has been doing since that era. Iranian hostilities after the Iranian Revolution of 1978 developed into the tense relationship that exists today between the US and Iran. This resulted from the overthrow of a government that supported cordial ties with the United States and disgruntled Iranian citizens. Iran now funds organizations like Hezbollah, which the US State Department has designated as a foreign terrorist organization, in an effort to further its anti-Western ideology. The notion that Iran's actions might have disastrous repercussions shapes the US's foreign policy approach toward Iran. Iran has refused to take part in a United Nations proposal for the Middle East known as the MENWFZ (Middle East Nuclear Weapon-free Zone), and it is in breach of several anti-nuclear laws, including the Nuclear Non-Proliferation Treaty (Richards, 2015).

US- Israel Cyber Strategy

It is only recently that the Department of Defense (DoD) has provided an outline of its cyber security structure, which includes a number of different mechanisms in addition to procedures. We recently finished this framework. The unclassified summary of the Department of Defense's 2018 cyber policy identifies five key priorities. Creating a more dangerous Joint Force is the first step. This includes increasing the rate at which cyber capacity is created, innovating what is already in place, utilizing intelligence to increase efficacy, and utilizing commercially available off-the-shelf software to remain secure when needed. The second goal is to continue fighting in cyberspace in order to uphold our motto, "peace through strength," which was first stated by Ronald Reagan, the 40th President of the United States. This entails lowering the probability that an enemy (a nation or an organization) will act hostilely, bolstering the durability of the vital infrastructure of the United States, and deterring enemies from taking harmful action.

Strengthening current partnerships and looking into the possibility of developing new ones is the third goal. This entails cooperating with foreign

partners to develop joint cyberspace operations, forming alliances within the private sector—which is in charge of much of the infrastructure in the United States—and abiding by the global standards for cyberspace. Redesigning the Department of Defense's guiding principles is the fourth goal, and part of that involves making cyber awareness one of the organization's main tenets. These objectives show how the Department of Defense is making more investments in cyberspace and how cybersecurity issues are now a top priority for the country (Dod Zero Trust strategy, 2021).

The department's fifth and final goal is to develop talent by boosting cyber talent and guaranteeing career advancement for cyber personnel. These objectives also show how cyber security issues have taken center stage in national security thinking. Apart from the Department of Defense's cyberspace investments, other government branches have also established laws to promote American involvement in cyberspace. By means of several legislative measures, including the National Defense Authorization Act of 2019, the United States is skillfully arranging itself to carry out offensive preventive cyber operations. This deed accomplished two goals:

(1) It made cyber-surveillance a "traditional military activity," and

(2) It granted the power to stop and neutralize cyberattacks by enemies like Iran.

The National Security Presidential Memorandum, a cyber-operation strategy outlining the objectives of forward defense, was drafted by the outgoing US president, Donald Trump. The Cybersecurity and Infrastructure Agency Act, which was also signed into law by the former president in 2018, renamed the National Protection and Programs Directorate of the Department of Homeland Security as the Cybersecurity and Infrastructure Security Agency and appropriated funds. It basically gives the go-ahead to employ offensive cyber operations (Dod Zero Trust strategy, 2021).

Iranian Cyber Strategy

The Iranian government has been active in the online community. They belong to a small group of nations that have extremely high organizational and strategic capabilities with regard to the cybersphere, despite not being among the most developed in terms of cyber capabilities. In 2017, even an Israeli general admitted that "they are not the most powerful superpower in the cyber dimensions, and they are not state of the art, but they are becoming better and better." Iran has stepped up its cyberattacks to a higher level of sophistication and scope in an effort to rile up its adversaries and defend forward, an offensive approach to national security. Iranian cyber tactics have changed over the last ten years, moving from straightforward website vandalism to more damaging assaults. Denial of service attacks, which prevent users from accessing network resources, and hard drive destruction are examples of these attacks. Iran has demonstrated a readiness to devote resources to enhancing its cyber capabilities. Iran is the ideal example of a nation that is rapidly developing its cyber capabilities to match the power of its adversaries and has high intentions of using them (Lewis, 2019).

Iran does not prioritize defense or deterrence. Iran is rapidly advancing its cyber capabilities to match those of its adversaries. Cyberattacks are typically carried out as a form of revenge or coercion. Iran's priorities include regional targets in the Middle East, especially Saudi Arabia, in addition to Western adversaries like the United States. Various types of attacks are conducted against these targets, irrespective of whether they are American, Saudi Arabian, or another type of target. An example of a normal cyberattack is the one that the Iranian hacker group conducted in 2019 against LinkedIn users connected to Middle Eastern government, banking, and energy companies. Another instance of a regular and typical attack occurred in 2019 when an Iranian espionage cell targeted digital infrastructure used by the US government, the Saudi Arabian government, and private industry. Multiple government strikes are less frequent, though. In 2012, Iran started attacking the US and its allies with the help of the Shamoon virus. The malware was created with Saudi Arabian and Qatari oil companies in mind. Three-quarters of the business computers of Saudi Aramco, the Saudi petroleum company, and Tasnee, the Saudi petrochemical company, were destroyed when their hard drives were erased. The malicious software also targeted other countries in the Middle East, including Kuwait and the United Arab Emirates. During this period of time, malicious software targeted

financial institutions in both the United States and Europe (Lewis, 2019b).

The American and Iranian Objectives in the Ongoing Cyber Conflict

In the digital realm, relations between the two countries have been increasingly tense over the course of the past decade. Both nations view this region as being critical to the success of their respective counterstrategies in this conflict. The use of computer simulations as opposed to actual physical combat is becoming increasingly popular. Because of Cyberspace tensions have the capacity to get out of hand due to a lack of deterrence and a disregard for rules and regulations. The failure to act as a deterrent and disregard for laws and regulations are both reasons why conflicts in cyberspace have the ability to spiral out of control, which should be understood in order to comprehend how aggressive the nature of cyber warfare is. The first reason that conflicts in cyberspace have a tendency to escalate into hostile conduct is the lack of any kind of deterrence within the domain. According to the theory of deterrence, any potential benefits of going to war are greatly outweighed by the risks. No country would willingly participate in hostile military action as a result. A fundamental component of both American and even Iranian foreign policy is deterrence. Although deterrence has kept the US and Iran from going to nuclear war, the overwhelming body of research indicates that deterrence does not exist in cyberspace.

Deterrence can be rendered ineffective due to its global reach, scattered nature, and interconnectedness, as per research published by the National Defense University Press. Because there is no deterrence in cyberspace, this suggests that the US and Iran could theoretically engage in a free and unrestrained conflict in this domain. Escalation happens a lot of the time. The second problem is that, despite having set some standards for themselves, neither Iran nor the United States of America initially adhered to them. The nations that have signed on to the North Atlantic Treaty Organization (NATO), most notably the United States, have developed a doctrine known as the "Allied Joint Publication". This doctrine lays out the fundamental rules for appropriate behavior in cyberspace. These codes of conduct aid in determining the nature of the threat facing NATO, the characteristics of offensive and defensive cyber operations, and the legal factors that must be taken into account when determining how to respond. In their version of the Allied Joint Publication, the Iranian Armed Forces issued the "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to Cyberspace." It states that both states have repeatedly disregarded their own rules and requirements in the event that Iran's sovereign leaders violate international law in cyberspace. The lack of any kind of deterrence and a general disregard for it has led directly to devastating attacks. For instance, in 2018, former president Donald Trump increased the Central Intelligence Agency's global cyberattack capabilities, enabling it to target not only government targets but also non-governmental infrastructure (Schmitt, 2020).

Iran is the opposing party in the conflict and is in charge of its own cyberattack against the US government. Seyed Abbas Mousavi, Iran's foreign minister, declared that the United States was responsible for a number of attacks on Iranian infrastructure and promised "legitimate defense and proportionate and suitable response to the aggression." Iran was in charge of its own cyberattack against the USA on the opposing side of the dispute. The Iranian government hackers known as APT attempted, but were unable, to spread password-spraying attacks against the US electrical grid. This is just one example of the many Iranian cyber-attacks that have attempted to damage or gain access to American infrastructure. Other Iranian cyber-attacks include those that have targeted the American financial system (Schmitt, 2020b).

Recommendations

With the prevalence of cyber warfare and the evolving tactics of adversaries like Iran, it's crucial for governments, especially the United States and its allies, to continuously enhance their cyber defense capabilities. This includes investing in advanced cybersecurity technologies, conducting regular cyber drills and exercises, and fostering collaboration between government agencies and the private sector.

Efforts should be made to reduce the risk posed by cyber warfare and to promote the establishment

of international standards and codes of practice in cyberspace. This includes advocating for the adoption of cyber standards that prohibit malicious cyber programs targeting critical infrastructure, the electoral process and civilians Diplomatic and multilateral forums play a role, especially in developing these programs.

Building a competent cyber staff is essential to successfully combat cyber threats. Governments and organizations should invest in cyber talent development programs, cyber security education, and training programs to develop cyber security professionals who can meet the evolving cyber challenges.

Timely actionable reporting is essential to identify and effectively mitigate cyber threats. Shared intelligence and cooperation between relevant agencies, both domestically and internationally, should also be prioritized to improve situational awareness and facilitate rapid response to emerging cyber threats.

In addition to technical strategies, addressing the underlying geopolitical tensions and grievances that fuel cyber conflict is essential for the long-term stability of cyber Interstate diplomacy efforts aimed at defusing tensions, encouraging dialogue, and resolving conflicts through peaceful means can help reduce the potential for cyber-warfare

Increasing public awareness and understanding of cyber threats is critical for building a cyber-resilient society. Governments, educational institutions, and the private sector should collaborate to raise awareness about cybersecurity risks, promote good cyber hygiene practices, and empower individuals to protect themselves against cyber threats.

Conclusion

On a worldwide scale, the problem of cyber risks and remedies has become more important in the literature, practice, and legislation imposed by governments. The dangers of the internet extend well beyond the realms of government, society, and private industry. As the world continues to become more digital and the economy becomes more interdependent, cyberspace is progressively becoming the platform through which state advancement will take place. This is due to the fact that the world as a whole is getting more digital. As the frequency and sophistication of threats continue to rise, nations are paying increased attention to the cyber laws and policies they have in place. The United States of America, Israel, and Iran are each working to improve the domestic and international connectedness of their respective nations through the use of cyberspace. These cyber dangers are getting greater, and they are increasingly directed at more complex tactics to offer ultimate damage to a state, as an example of this can be seen in the case of Iran with the Stuxnet attack, which severely damaged Iran's nuclear enrichment facility in Natanz.

Hackers may target military databases, for instance, in order to gather information about troop movements and the handling of weapons and equipment. These assaults can also target other state institutions; therefore, the military and other state institutions are not immune to them. In this research, the counterstrategies that Iran ought to implement in order to deal with these cyber challenges and hazards were described. The level of cyber threats is expected to keep rising as a direct result of Iran's forward progress and expanding online presence. Therefore, Law, policymaking, coordinated efforts, and community accountability are also required in order to secure Iran's digital domain. In conclusion, it is reasonable to claim that, particularly for those states that have advanced enough, a combined knowledge of the technical aspects of cyber security and the viewpoint provided by the humanities are currently of the greatest importance to national security. This is particularly true for states where living standards are higher than average. Numerous instances, such as the numerous cyberattacks that have occurred recently, lend credence to this assertion. Consequently, cyber security is a crucial component of national security that necessitates a deep and comprehensive comprehension.

References

Al Jazeera. (2024). *US sanctions hundreds of individuals, firms over Russia's war in Ukraine*. https://www.aljazeera.com/economy/2024/5/2/us-sanctions-hundreds-of-individuals-firms-over-russias-war-in-ukraine
Google Scholar Worldcat Fulltext

Aminloo, R., &Vitone, T. (2022). *Cybersecurity policies and International Relations: The case of the US and Iran*. Journal of Student Research. https://www.jsr.org/hs/index.php/path/article/view/2666
Google Scholar Worldcat Fulltext

Antunes, S., & Isabel. (2018). *Introducing realism in international relations theory*. E. https://www.e-ir.info/2018/02/27/introducing-realism-in-international-relations-theory/
Google Scholar Worldcat Fulltext

Baram, G. (2022). *Analysis | how the cyberwar between Iran and Israel has intensified*. The Washington Post. https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/
Google Scholar Worldcat Fulltext

Craig, A., &Valeriano, B. (2018). *Realism and cyber conflict: Security in the Digital age*. E. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/
Google Scholar Worldcat Fulltext

Cyberterrorism: How real is the threat?. United States Institute of Peace. (2015). https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat
Google Scholar Worldcat Fulltext

DodZero Trust strategy. (2021). https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
Google Scholar Worldcat Fulltext

Dykstra, J., Inglis, C., & Walcott, T. S. (2020). *Differentiating kinetic and cyber weapons to improve integrated combat*. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2421554/differentiating-kinetic-and-cyber-weapons-to-improve-integrated-combat/
Google Scholar Worldcat Fulltext

Epps, G. V. (2013). *Common ground: U.S. and NATO engagement with Russia in the Cyber Domain U.S. and NATO engagement with Russia in the cyber domain on JSTOR*. Jstor. https://www.jstor.org/stable/26326340
Google Scholar Worldcat Fulltext

Fischer, M. (2019). *The concept of deterrence and its applicability in the cyber domain | connections: The Quarterly Journal*. Jstor. https://connections-qj.org/article/concept-deterrence-and-its-applicability-cyber-domain
Google Scholar Worldcat Fulltext

Hanna, A. (2023). *The invisible U.S.-Iran cyber war*. The Iran Primer. https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war
Google Scholar Worldcat Fulltext

HARE, F. (2010). The cyber threat to national security: Why can T we agree? https://ccdcoe.org/uploads/2018/10/Hare-The-Cyber-Threat-to-National-Security-Why-Cant-We-Agree.pdf
Google Scholar Worldcat Fulltext

Irandoost, D. H. (2018). *Cybersecurity: A national security issue?*. E-International Relations. https://www.e-ir.info/2018/05/03/cybersecurity-a-national-security-issue/
Google Scholar Worldcat Fulltext

Jr., S. U., & Arnold, C. (2023). *Cybersecurity is critical for all organizations – large.*
Google Scholar Worldcat Fulltext

Lewis, J. A. (2019). *Iran and Cyber Power*. CSIS. https://www.csis.org/analysis/iran-and-cyber-power
Google Scholar Worldcat Fulltext

Lewis, J. A. (2019b). *Iran and Cyber Power*. CSIS. https://www.csis.org/analysis/iran-and-cyber-power
Google Scholar Worldcat Fulltext

Li, Y., & Liu, Q. (2021). *A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments*. Energy Reports. https://www.sciencedirect.com/science/article/pii/S2352484721007289
Google Scholar Worldcat Fulltext

Ministry of Foreign Affairs (China). Reality check: Falsehoods in US perceptions of China. (n.d.). https://www.fmprc.gov.cn/eng/wjbxw/202206/t20220619_10706059.html
Google Scholar Worldcat Fulltext

Richards, A. M. C. (2015). *Iran as a strategic threat to the U.S. in the Middle East and its impact on U.S. policy in the region*. https://bearworks.missouristate.edu/theses/1502/
Google Scholar Worldcat Fulltext

Schmitt, M. N. (2020). *Noteworthy releases of International Cyber Law Positions-Part II: Iran.*

Lieber Institute West Point. https://lieber.westpoint.edu/iran-international-cyber-law-positions/
Google Scholar Worldcat Fulltext

CISSP-ISSAP, M. (2021). *What Is Cyber warfare?*. Security information, news and tips from TechTarget. https://www.techtarget.com/searchsecurity/
Google Scholar Worldcat Fulltext

Staff, A. J. (2022). *US imposes new sanctions on Iran over Albanian cyberattack*. https://www.aljazeera.com/news/2022/9/9/us-imposes-new-sanctions-on-iran-over-albanian-cyberattack
Google Scholar Worldcat Fulltext

What is cyber warfare: Types, examples & mitigation: Imperva. Learning Center. (2023). https://www.imperva.com/learn/application-security/cyber-warfare/
Google Scholar Worldcat Fulltext