Journal of Research in Social Sciences (JRSS)
Vol No 12, No 02, July 2024.pp42-62
ISSN: 2306-112X(E); 2305-6533 (P)
https://doi.org/10.52015/jrss.12i2.271

Cyber Security Threats to Iran and its Countermeasures: Defensive and Offensive Cyber Strategies

Syed Qandil Abbas[1], Hareem Fatima[2]

Article History:

Received:

April 10, 2024

Accepted:

July 04, 2024

Published:

July 15, 2024

Funding:

This research received no specific grant from any Public, Commercial or not for profit sectors.

Abstract

Iran's convoluted geopolitical status, its centrality to locale-specific wars, plus the shifting balance of the global order make cyber security a key issue worldwide in addition to traditional security challenges. Iran is an appealing target for cyber enemies due to its numerous security vulnerabilities, which include ransomware infection, scams, as well as complicated malware. Iran has taken a flexible stance, via collaboration, authorized, and intellectual tactics to counter these concerns. Forming cyber security teams, utilizing the latest innovations, and hiring competent employees are all examples of efforts in cyber defense. Legislative structures are essential for bringing criminals before the law and discouraging unlawful behaviour, but the dynamic nature of cyber threats makes it difficult to update rules. The goal is to keep information security and safety measures under check. The identification and mitigation of cyber dangers necessitate collaboration with various nations, global organizations, and corporations. Iran's cyberspace involvement shapes societal sentiment and upholds the will of the people, with both advantageous and hazardous repercussions. To bolster its application and balance its powerful adversaries, it employs cyber assaults in conjunction with conventional asymmetrical combat strategies. What is Iran's main cyber security concerns and challenges, and how is Iran addressing as well as tackling them, is the question that this study aims to answer.

KEY WORDS: Iran, cyber threats, asymmetric warfare, guerrilla warfare, ransomware

[1] Dr Syed Qandil Abbas with special focus on the Middle East, is associated with School of Politics and International Relations, Quaid-e-Azam University Islamabad, syed572@hotmail.com

[2] Hareem Fatima is an MPhil Scholar of International Relations with Special Focus on Cyber Security at Quaid-e-Azam University Islamabad, hareem.fatimah786@gmail.com

Introduction

Cyber security is comparatively a new apprehension for peace and stability which is consequently instigating diverse counter strategies. It is the discipline of defending programmes, networks, and systems from online threats along with several opportunities. Typically, the goals of cyber-attacks are to disrupt regular corporate operations, obtain, alter, or delete sensitive data, or use ransomware to demand money from customers. Cyber security encompasses all facets of preserving a company, its personnel, and its resources against online dangers. Geopolitical upheaval combined with rapid technology progress has resulted in an increase in cyber security concerns for countries like Iran. The purpose of this study is to evaluate Iran's cyber security environment by looking at the different cyber threats that the country's government, corporate community, and critical infrastructure must contend with. Iran's resistance to cyber-attacks is assessed, along with the efficacy of its present cyber security schemes, procedures, and technology initiatives. Iran's counterstrategies are also evaluated. For several reasons, it is imperative to evaluate Iran's defences and analyse the country's cyber security risks. It can assist in strengthening defences, enhancing awareness of new cyber threats, and locating vulnerabilities in Iran's technological infrastructure (“What Is Cybersecurity?” 2024b). In addition to educating policymakers and encouraging international cooperation to counter shared cyber threats, this study may suggest modifications to national cyber security laws. This study will explore that what emerging cyber security threats could pose new challenges to Iran and what are the rising cyber security strategies and counter-strategies of Iran?

Literature Review

Although there is a lot much literature on the issue of Iran and cyber security but very limited sources are addressing this issue in expounding sense. One of the scholars, David E. Sagner in his article "Obama Order Sped Up Wave of Cyber-attacks Against Obama Order Sped Up Wave of Cyber-attacks Against Iran published on June 1st, 2012 highlights that Obama used the Stuxnet virus to undertake a clandestine cyber-attack against Iran that seriously damaged its nuclear centres and signalled a major uptick in American digital warfare (David E. Sanger, 2012). Another book "Cyber War Will Not Take Place" by Thomas Rid outlines the case that actual cyber warfare—which frequently resembles sabotage, espionage, or subversion—is unlikely to occur and emphasises the need to distinguish cyber-attacks from conventional warfare (Rid, 2012). Another scholar Kim Zetter in his book "Countdown to Zero Day" explores the creation and consequences

of Stuxnet, the first digital weapon ever discovered, as well as the continuous threats posed by cyber-attacks (“Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon,” n.d.). Scholars Collin Anderson and Karim Sadjadpour in their book "Iran’s Cyber Threat: Espionage, Sabotage, and Revenge" argues that Iran's cyber threat is a grave risk to global cyber security because it involves advanced espionage, sabotage, and retaliation (“Iran’s Cyber Threat,” n.d.-b). Thus, grasping its strategies is crucial for formulating efficacious countermeasures.

A complex topic of study, Iran's cyber security landscape has research gaps/deficiencies in fields such as collaborating globally, domestic cyber security regulations, cyber skill acquisition, and hiring and training of the nation's cyber employment. Iran's technology expenditures, cyber security setup, and protocols for detecting and thwarting cyber-attacks all needs to be carefully reviewed. Iran's defences in opposition to foreign cyber threats also need to be thoroughly evaluated. Fixing up these voids will allow researchers to have a better understanding of the threats it faces and the strategies it employs to avoid them.

Theoretical Framework: Securitization Issue and Cyber Realism Theory

A theory of politics called securitization seeks to provide insight into how people make social obligations, recognise societal issues, and come up with alternative options. It has evolved over the past decade and is unique in its ability to describe a specific security strategy shaped by the speech act using an "analytics of government" approach that prioritizes procedures and practices. This issue faces three theoretical, methodological, and methodological problems. The core tenet of securitization issue is that a problem is made salient enough to garner public support, allowing those in charge to employ whatever tactics they consider fit. It blends the political aspects of threat mitigation with threat design. Key ideas of securitization issue include the securitizing agent, referral matter, referential item, viewers, setting, and acceptance of particular regulations (Eroukhmanoff, 2020b).

Iran is vulnerable for external assaults and domestic weaknesses that pose serious cyber security risks. The Iranian government and security services, including the Islamic Revolutionary Guard Corps, portray threats as existential risks to the country's stability, security, and sovereignty. Iranian officials often emphasize the risks of cyber-attacks in public remarks, defending the investment of funds in cyber security and the enforcement of stringent regulations. Examples of securitization in

Iranian cyber security include cyber-attacks and espionage justifying widespread state monitoring and control over internet usage, as well as the Stuxnet Incident targeting Iranian nuclear facilities. Securitization theory provides a framework for examining Iran's reaction to cyber security risks, as the Iranian government justifies significant steps to safeguard national security by portraying these challenges as existential risks (Jammal, 2023).

The article uses Cyber-Realism theory to analyse the digital conflicts and rising threats towards Iran. The widespread use of advanced technologies like the Internet has led to conflicts between state, illegal, and political parties in cyberspace. Iran's reliance on electronic networks for information and data transfer can be disrupted if critical infrastructures fail. The automation of procedures and data concentration on computers has improved business and state revenue but also created security issues. Digital financial surveillance can lead to theft of military equipment and scientific advancements, making Iran more vulnerable to cyber-attacks and exploitation. Cyber realism theory examines the relationship between society, politics, and technology, highlighting the influence of artificial intelligence (AI) on world politics. AI blurs the lines between real and virtual worlds, affecting power dynamics, cyber security regulations, and international politics. AI integration improves identification, reaction, and mitigation operations, enabling rapid threat prevention through large data analysis and machine learning. AI automates security tasks, freeing up cyber security experts to tackle complex issues. The purpose of using this theory is to assess the contribution of Cyber-Realism theory for understanding the rising cyber security threats towards Iran and Iran's countermeasures (Marcio Rocha and Daniel Farias Da Fonseca, 2019).

Emergence of Cyber Security: Historical Background

The term "hacker" is often associated with a shadowy figure, but the term "modern hacker" first emerged from the counterculture of individuals experimenting with technology and developing novel information-sharing strategies. Cybercrime has evolved significantly since the first computers connected to the internet in the 1960s and 1970s, with hackers constantly developing new strategies for breaking in and gathering data. The field of cyber security emerged during the 1960s and 1970s, and gained widespread attention in the 1980s due to incidents that highlighted the consequences of inadequate security. The rise of the internet and the rise of data digitization led to more frequent attacks and data breaches. In the 2010s, the scope of threats grew, with nation-states launching more frequent attacks, conducting infiltration and surveillance operations, and

using cyber weapons to target strategic targets. In today's interconnected world, cyber security is just as important as technology, with hackers employing social engineering and emotional manipulation to breach secure systems (Codecademy, n.d.). Securitization theory clarifies the framing of issues as security threats, which is pertinent to the history of cyber security since it shows the transition from considering cyber threats as technical issues to matters of national security. This progression highlights the growing importance and distribution of resources in the fight against cyber threats.

Cyber-Security Challenges

Cyber security is becoming increasingly important for businesses, with supply chain attacks, ransomware, phishing attacks, and zero-trust security techniques being key threats. The evolution of malware has made traditional detection methods insufficient, and prevention-focused cyber security tools are necessary to reduce the threat posed by Gen V malware. Denial of service (DoS) attacks and zero-day vulnerabilities pose a serious threat to business cyber security. The global cybercrime issue is increasing, with a 28% rise in Q3 2022 compared to Q3 2021 (Michali, 2023). To protect against global threats, businesses must develop a robust cyber security program that includes constant monitoring, access to the latest threat intelligence, and comprehensive threat prevention. Weaponization of acceptable tools is crucial, as cybercriminals often use features found in target operating systems or accessible through trustworthy programs. Cloud computing is becoming more popular, but compromised knowledge of security guidelines and collaborative security models makes it more susceptible to intrusions than on-premises equipment (Jnguyen, 2023). Since cyber security risks are frequently perceived as serious security dangers necessitating extraordinary actions, securitization issue and cyber-realism theory has become vital for understanding these challenges.

Cyber Security and its Relevance with Artificial Intelligence (AI)

AI's ability to analyse unstructured data, figures, voice patterns, and words can save time and money, making it increasingly used by industries, private sector businesses, and government agencies. However, AI has weaknesses, as hackers often attempt to access systems through undiscovered vulnerabilities, leading to data breaches and the loss of private information. AI can also gather information while waiting for an unauthorised user to become clumsy to look for known attacker behaviours. As hackers adapt to AI systems, programmers must implement new

protective techniques. Neural Structured Learning (NSL) is an open-source framework developed by Google that uses the Neural Graph Learning approach to develop records and data patterns in neural networks. It can execute natural language processing (NLP), render machine vision models, and project data from interactive databases. Better prediction performance can be achieved when organized signals are used during training, especially when there is limited data (Trung Tran, 2022).

AI has provided tools for facial identification, search engines, speech recognition, payment card companies, and investment firms to prevent fraud. By improving the assessment, analysis, and comprehension of cybercrime, AI has the potential to transform data security for enterprises. However, AI can also be highly resource-intensive and a powerful tool for cybercriminals who use technology to enhance their attacks. Ultimately, AI has the potential to transform data security for companies by improving assessment, investigation, and understanding of cybercrime. However, when applying AI techniques to cyber security, it is crucial to differentiate between short-term goals and long-term perspectives ("Artificial Intelligence in Cyber security: Pros and Cons," n.d.). Artificial intelligence and cyber security are major security concerns that call for drastic measures and legislative actions to defend against alleged threats. Cyber-Realism theory along with the securitization concept is essential in tackling these challenges.

Positive and Negative Impacts of Cyber Security

Cyber technology has several benefits, such as cost savings, ease of use, efficiency, innovation, worldwide connectivity, and information access. It increases overall efficiency by automating jobs, streamlining workflows, and enabling speedier communication. It promotes international ties and makes instantaneous communication and teamwork possible. Innovation is further stimulated by cyber technology, which offers a platform for fresh services, products, and business ideas. It gives people and organisations access to an unprecedented amount of knowledge, enabling them to make informed decisions. Through automation and digitization, it can also lower expenses related to travel, physical infrastructure, and human operations (Saxena, 2024).

Cyber technology creates new points of vulnerability that expose people and companies to online dangers such as malware, phishing, hacking, and data breaches. The gathering, storing, and usage of sensitive information by businesses and governments give rise to privacy concerns. The digital divide is made worse by cyber technology, which makes the difference between those who have

accessibility to technological advances and those who do not grow. Overly dependent on cyber technology can cause crucial systems to become vulnerable, disrupted, or even fail catastrophically. Cyber technology-driven automation may result in job displacement and necessitate the acquisition of new skills by workers. Identity theft, internet fraud, and cyber-extortion are examples of cybercrime that has increased (Roberts, 2024). Securitization concept and cyber-realism theory examines the framing and addressing of cyber security concerns, emphasising both proactive security measures and unfavourable outcomes such as creating fear or securitizing non-security matters.

Cyber Security Threats to Iran: Historical Overview

Since the 1979 revolution in Iran and the founding of the Islamic Republic, Iranian leadership has been at odds with the West and Middle Eastern neighbours. The hostage crisis following the United States' relationship with the deposed Pahlavi monarchy laid the groundwork for future tensions between the two countries. Economic sanctions, legal action, and diplomacy have been used by the US and its allies to limit, oppose, and weaken Iran's power. The West's rising anxiety over Iran's military aspirations, including strategic cyber-attacks, has been compounded by the country's drive to build its status as a nuclear power (“The Iranian Cyber Threat,” n.d.).

In 2010, an intricate cyber-sabotage operation aimed at Iran's nuclear facilities in Natanz proved crucial for the U.S.-Islamic Republic relationship. Many people alleged that U.S. and Israeli intelligence were behind the operation, despite the U.S. administration never acknowledging responsibility for the Stuxnet virus. Iran quickly built up its cyberspace capabilities after the Stuxnet assaults, leading to a major explosion that damaged the internal electrical system that powers Iran's subterranean uranium enrichment centrifuges and caused a blackout at the country's nuclear facility in Natanz. Israel and Iran are notorious for their enduring historical hostilities and tit-for-tat attacks, and there is a good chance that Iran may use cyberspace as an attack vector in response to the recent sabotage it accuses Israel of committing. The United States finds itself in a difficult position, as it wants to salvage the nuclear deal but is hesitant to openly denounce its longstanding partner. If Iran launches a cyber-attack against the United States, it is likely to target American government, commercial institutions, and vital industries like energy, finance, healthcare, and shipping (“Analysis of the Iranian Cyber Attack Landscape,” 2021). Securitization issue in addition with cyber-realism theory explains how threats are created, validated, and shaped

into policies and actions, which is important information to know when analysing cyber security hazards to Iran.

Cyber Security Threats to Iran

Threats associated with cyber security are dynamic and can vary over time, as can the nature and intensity of cyber-attacks against countries such as Iran. The first prominent cyber-attacks targeting Iran were caused by the 2009 crash and vandalism of Twitter's main page, the 2010 Stuxnet virus infection of computers at the Bushehr nuclear power plant (which was allegedly developed by the US and Israel), and the explosions that followed in the IR-1 centrifuge engines in Natanz. After looking into the virus, Iran held the US and Israel responsible. With 30,000 computers infected by Stuxnet, the Atomic Energy Organisation of Iran (AEOI) said in September 2010 that it was fighting malware targeting its nuclear plants (Institute for Political and International Studies, n.d.-b).

The third malware, Duqu, was discovered in November 2010 by Iran with the intention of interfering with Iran's nuclear project. The Stuxnet attack also used the same programming code as Duqu. Iran's cyber defence agency discovered the "Stars" malware in April 2011, which mimicked official government files and caused "small harm" to computer systems. Iran held the United States and Israel accountable. Iran discovered in April 2012 that the "Wiper" malware, which looked like Duqu and Stuxnet, was erasing hard drives on computers under the authority of the oil ministry and the National Iranian Oil Company. Iran blamed the US and Israel for the attack (Ifmat, 2019). Since cyber threats are treated as security concerns, securitization and cyber-realism theory examines how problems are seen as security threats.

Turning Point in Iranian Nuclear Installations: The Olympic Games Operation

Operation Olympic Games was probably an effort by the US and Israel to destroy Iranian nuclear facilities via cyberspace. One of the earliest known offensive cyber weapons was this one. President Obama hastened the 2006 initiation of the cyber-attack on the nuclear facility in Natanz, following President George W. Bush's recommendation to keep up the cyber-attack in order to avert a conventional Israeli assault (Kamiński, 2020).

This operation is comprised of viruses that are as follows:

A. Stuxnet (2010)

The 2010 discovery of the sophisticated computer worm Stuxnet led to significant disruptions to Iran's nuclear installations, particularly its facilities for uranium enrichment. Stuxnet was created as a cyber-weapon targeting industrial control systems, such as PLCs, used in Iran's nuclear programme. The worm exploited security gaps within industrial control infrastructure, including those used in Iran's nuclear plants, by compromising PLCs responsible for centrifuge operations using zero-day attacks, harmful software injections, and advanced tactics. Its ability to avoid detection and spread covertly over networks sealed off from outside interference highlighted the inherent susceptibilities of vital infrastructure to cyber-attacks. The worm also disrupted the centrifuge process by sending unauthorised commands to PLCs, controlling their speed and functionality, causing them to malfunction or spin at strange speeds. Evidence suggests that state entities, possibly including Israel and the United States, may have participated in the creation and use of Stuxnet as a clandestine cyber weapon. The effectiveness of Stuxnet in undermining Iran's nuclear installations demonstrated the seriousness of cyber-attacks in real-world infrastructure and the capabilities of strategic adversaries. Iran took action to control and lessen the impact of the Stuxnet malware, strengthening cyber security defences, separating important systems from outside networks, and conducting extensive security audits and inspections (Fruhlinger, 2022).

B. Duqu Virus (2011)

In 2011, Duqu, a sophisticated malware, was discovered and used to target Iran's vital networks and industrial control systems. Unlike Stuxnet, Duqu was primarily used for intelligence gathering and espionage, stealing confidential information, intellectual property, and sensitive data. It posed a significant threat to national security and commercial interests in Iran by infiltrating government institutions, industrial automation systems, and vital infrastructure networks. The malware's persistence and stealth capabilities made it difficult to identify and eliminate from compromised systems. Evidence suggests Duqu is connected to state-sponsored espionage operations aimed at Iran's vital infrastructure and resources. The discovery underscores the importance of strong cyber security defences, intelligence sharing, and international collaboration in combating these threats (Bencsáth, Pék, Buttyán, & Felegyhazi, 2011).

C. Flame Virus (2012)

The Flame virus, a highly developed form of malware with features such as network mapping, stealing data, control and command, and infection mechanisms, was discovered in 2012. Since at least 2010, it is believed that hackers have mainly target Iran alongside other Middle Eastern countries. Flame looks to have been developed by a nation-state more for information gathering than for actual physical harm. The impact of cyber-espionage on Iran has led to inquiries into the extent and efficacy of such activities against Iran and other countries in the area. Governments and security firms worked together to understand the design and features of Flame, and security patches and updates were made accessible to lessen vulnerabilities that the virus took use of (Lee, 2012).

China-Russia-Iran: A Tripartite Cyber Cooperation

Iran's MP, Abolfazl Moue, supports the 25-year strategic partnership deal between Russia and Iran, claiming that Russia is helping Iran with cyber security. The pact aims to tighten information security protocols, combat cyber threats, and promote bilateral collaboration. It includes provisions for information sharing and cooperative prosecution of criminal offenses between Russia and Iran. Western countries and their supporters are concerned about Tehran and Moscow's strengthening military, political, interactions, and cyber relations. Hacker groups have often targeted Iran's government networks, with the frequency of attacks growing after the 2022 revolt. State-sponsored hacking groups, such as those associated with Iran, frequently use Russian underground forums, which have unrestricted funds and may devote a substantial amount of cash purchasing malware (Pfneisl, 2023). Microsoft revealed in February 2024 that hackers with state support from China, Russia, and Iran have been using technologies designed by Microsoft-backed OpenAI to improve their cyber espionage skills. The growing friendship between Tehran and Moscow may lead to a more official engagement in the cyberspace. Iran has already received surveillance gear, intelligence tools, covert photographic equipment, and lying detectors from Russia. Rumors suggest that Moscow may have given Tehran access to cutting-edge software, allowing Iranian officials to break into political dissidents' and oppositionists' phones in 2022. The 25-year strategic partnership deal in January 2022 focuses on cyber security, including China's help in setting up a private Internet in Iran (Figueroa, 2023). Securitization and cyber-realism theory places an emphasis on socially manufactured security challenges, which have an impact on governments' actions to resist perceived common dangers and the cooperation of the China-Russia-Iran tripartite alliance.

National Cyber Security Strategy of Iran: Importance of Cyber Strategy

Iran has been using asymmetric warfare since the final days of the 1980–1988 Iran–Iraq War as a major component of its national security strategy. The officers of the IRGC who fought in the war and still make up the backbone of Iran's military hierarchy were influenced by this tactic in their outlook on life. Iran's hegemonic strategy as a progressive regional power is based on eliminating Western influence in the Middle East and advancing its philosophy of Islamic revolution based on "anti-Imperialism". Iran's conventional military might is weaker than that of its enemies, the United States, and its allies in the Middle East, which puts it at a disadvantage. Despite these structural drawbacks, Iran has managed to forge small spheres of military, diplomatic, and political influence in surrounding nations rather than depending on asymmetric methods ("The Iranian Cyber Threat," n.d.).

Iran has developed relationships with anti-US and Israel groups and militias to establish dependable partners and cause influence in surrounding countries, granting it considerable power in Yemen, Syria, Iraq, Lebanon, and other regions. To offset the lack of long-range attack capacity in its air force, Iran has also built an advanced drone programme and accumulated the biggest and most varied ballistic missile stockpile in the Middle East. Iran's acquisition of cyber warfare features is a powerful complement to its asymmetric arsenal, providing it with low-cost means beyond its restricted conventional capabilities to carry out espionage against and attack more powerful adversaries in support of its foreign policy along with national security goals (Rodriguez-Hernandez & Velásquez, 2021).

Iran can cause significant harm to enemies' economy and national security through cyber-attacks, which also lessen the possibility of a kinetic reaction and usually provide some degree of attribution with denial over the attack's source. The comparatively level playing field in the cyber warfare sphere is another draw, and Iran has led the way in showcasing the ability of smaller players to challenge superpowers. Iran might, however, find it challenging to carry out its own significant cyber-attacks against the American government, the armed forces, the biggest banks and companies, the most vital industrial control systems, and other high-value targets ("The Iranian Cyber Threat," n.d.). Iran approaches cyber security as a matter of national security and the securitization notion plus cyber-realism theory helps to shape its actions in this regard.

Iran Cyber Security Strategy and the Use of AI

Iran, a Middle Eastern nation with a rich history of invention, is a regional leader in technology. It has invented windmills, irrigation systems, and ventilation systems dating back to the Achaemenid Empire. Iran initiated nuclear technology development during Mohammed Reza Pahlavi's rule, initially for domestic energy production and later for nuclear weapons. The Sharif University of Technology was established in 1966, setting the stage for civilian technology developments. Iran's contribution to technology increased from 3.8% of GDP in 2016 to 6.9% in 2020 (Lester, 2023). In 2021, Iran had approximately 6,300 scientific enterprises, compared to three thousand in 2016 (Lester, 2023). The country's educated shipments increased five times between 2014 and 2017. Iran is keen to capitalize on artificial intelligence advancements to establish its status as a leader in the field (Lester, 2023). The government plans to be at the forefront of the global market by 2032. Iran launched two AI-powered navigational applications, BALAD and SURENA, to assist passengers in finding suitable travel routes and selecting top destinations for entertainment, activities, and services. The country has outperformed Saudi Arabia and Israel in terms of its inventive start up ecosystem, with 400 businesses in Tehran alone since 2014 (Smith, 2023) . However, the government has not provided entrepreneurs with funding. Iran is expected to rank among the top ten countries in AI by 2032 (Smith, 2023). To maintain this trend, Iran needs continuous investment, teamwork, and an emphasis on ethical issues. The world is eagerly observing Iran's progress towards becoming a global leader in AI (“Iran Plans to Become a Leading Country in AI,” 2022). By viewing AI as a possible threat actor and affecting resource allocation and policy responses, the securitization and cyber-realism theory could influence cyber security tactics.

Iran’s Rising Cyber Security Strategy: Noteworthy Instances

There exists multiple cyber-attack incidents towards Iran; few of examples include (Tariq, 2024):

1. Three nuclear experts perished in Tehran in January 2010, and Israel and the US were blamed for the attacks.
2. A nuclear engineering professor perished in an automobile explosion in November 2010, and a chemical engineering graduate perished in January 2012.
3. Mohsen Fakhrizadeh regarded as the chief of Iran's nuclear program was slain in November 2020 through allegedly Israel’s Artificial-Intelligence based attack.

4. Colonel Hassan Sayyad Khodaei was shot five times outside of his home in May 2022. Majid Mirahmadi said Israel was responsible for the crime.
5. Israel has been targeting Iran for a decade, accusing it of nuclear weapons development. The April13, 2024 attack sparked tensions during the Gaza War, but Iran disputes this and asserts peaceful nuclear energy use (Tariq, 2024).

As it's clear by its reaction to Stuxnet, Iran's cyber security policy is ostensibly based on securitization and cyber-realism perspective. Tehran considers cyber threats as serious challenge and justifies defence measures to exercise power over cyberspace. Discussed below are some of the prominent cyber-attacks concerned with Iran:

A. US Drone Hacking: Accusation Towards Iran (2009)

Hackers from Iraq have used software purchased online for $26 to harm US drones, revealing potential targets when they relayed live footage to a US controller (MacAskill, 2017). The US has increased the use of drones six fold in the last five years, making them a significant component of the US armament. Drones can fire missiles at suspected al-Qaida and Taliban terrorists in Afghanistan and the Pakistani border region, as well as suspected fighters in Iraq. If rebels knew which locations were being targeted, they may take evasive measures, which could pose an issue with the hacking. A US source confirmed the allegation, but a US source stated that the insurgents would not have gotten much use out of the images' quality. Drones in Pakistan are operated by the CIA, while those in Iraq and Afghanistan are under the control of the US air force. The Pentagon has been aware of the issue for years and is continuously assessing the efficiency and safety of its intelligence, surveillance, and reconnaissance (ISR) systems. Upgrading encryption in drones will take time due to thousands of ground stations and at least six hundred unmanned aircraft in operation. Video streams from a drone were discovered on the laptop of an insurgent in Iraq who was purportedly supported by Iran last year (MacAskill, 2017).

B. Iran Tried to Capture US Drone (2011)

An Iranian ship attempted to seize a US Navy sea-based drone in the Persian Gulf, but failed. The Iranian Revolutionary Guard Corps Navy (IRGCN) back ship Shahid Baziar seized and pulled the unsupervised sea container in a region that the US Navy's 5th Fleet patrols (BBC News, 2012). The USS Thunderbolt surveillance ship observed the Shahid Baziar towing the Saildrone Explorer,

which was equipped with detectors, radar systems, and cameras but did not hold any sensitive or classified data that the Iranians could have used. The US claims that the Iranians severed the tow connection and that the crew's professionalism and expertise stopped Iranian illicit activity. Decrypted video footage of Kandahar and a US outpost are allegedly depicted in decrypted video footage obtained through a US spying drone that was shot down in 2011. Iran has repeatedly charged the US of espionage in the on-going tensions around its nuclear program (BBC News, 2012).

C. Implementation of Face Recognition Technology: Mohsen Fakhrizadeh's Incident (2020)

Iran's top nuclear scientist, Mohsen Fakhrizadeh, was killed in a convoy outside Tehran on 27 November 2020 (BBC News, 2020). Brig-Gen Ali Fadavi claimed that a weapon mounted in a pick-up truck could fire at Fakhrizadeh without hitting his wife. Iran has blamed collusion between Israel and MKO, an exiled hostile group for the attack. A Nissan pick-up was said to have exploded at the scene. The head of Iran's Supreme National Security Council said it was a remote attack using "special methods" and "electronic equipment". Ayatollah Ali Khamenei has vowed to avenge the assassination and demanded the "definitive punishment" of those behind it (BBC News, 2020). Israeli public radio reported that Israeli security officials had warned some former nuclear scientists to be cautious. The claims made about the attack using such a sophisticated high-tech weapon are alarming and dystopian. The use of AI in conflict has been a concern for many scientists, with Stephen Hawking signing an open letter calling for a ban on the development of artificial intelligence for military use in 2015. (Jazeera, 2021).

D. Hitting of Iranian Fuel Tank Facilities (2021 and 2023)

Parviz Mohammadnezhad Ghazimahalleh, a member of Iran's Energy Committee, asserted that a cyber-attack targeting 70% of the nation's gas outlets was executed "from inside." The hacker collective "Gonjeshk-e-Darande," also known as Predatory Sparrow, claimed credit for the attack, claiming to have taken out "a majority of the petrol pumps throughout Iran" ("Iranian MP Says Fuel Cyber Attack Was Inside Job," 2023). "Gonjeshk-e-Darande" is accused by Iran of having ties to Israel. The incident occurs one day after another Iranian parliamentarian, Hadi Beigi-Nezhad, claimed that the gasoline system was contaminated by a cyber-virus. According to Tejarat News, most petrol stations in the province of Tehran have been linked to the internet distribution

network. Another Iranian politician, Morteza Mahmoudvand, accused Israel's intelligence service, Mossad, and "Zionists" of being behind the fuel system attack. He called for "an equilibrium of fear" in order to combat Iranian foes. The Islamic Republic has already taken part in other cyber-attacks against Israeli targets, including an Irish water facility (“Iranian MP Says Fuel Cyber Attack Was Inside Job,” 2023).

Iran’s Counter Strategies against Cyber Attacks: Traditional and Military Approaches

Iran has been engaged in numerous countermeasures against cyber-attacks from different countries. Some traditional and military cyber activities concerned with Iran includes APT33 (Elfin), Mabna Institute Indictments (2018), Operation Cleaver (2014), Oil Rig (APT34), Operation Ababil (2011–2013). Because of economic sanctions and cyber activities against Iran, these attacks were primarily directed on financial institutions in the United States (“Enhancing Iran’s Cyber security: Strategic Measures and Challenges,” 2024). The organisation used spear-phishing, stealing credentials, and distributing malicious software. Nine Iranians were charged by the US Department of Justice in 2018 for engaging in cyber espionage activities. Whereas APT33 concentrated on the aerospace, defence, energy, and petrochemical industries, Operation Cleaver targeted vital infrastructure across sixteen countries. These events demonstrate Iran's aggressive participation in cyber warfare. Cyber-attacks on Iran are ascribed to state-sponsored or military groups; they collect intelligence, interfere with vital infrastructure, and limit Iran's capabilities. Operation Olympic Games, Flame, Wiper, Operation Cleaver, and Triton/Trisis are a few instances that illustrate the geopolitical ramifications and regional concerns associated with current cyber warfare and espionage operations (“Enhancing Iran’s Cybersecurity: Strategic Measures and Challenges,” 2024). Understanding threat development and legitimation—which in turn shapes policy responses—is made possible by the use of securitization and cyber-realism theory, as both are essential for grasping Iran's cyber security tactics.

Iran’s Offensive Actions against Cyber Attacks

Iran's internet usage has evolved from internal control to active operations against foreign targets. To defend local networks, the Iranian experts have been creating indigenous internet infrastructure and cyber security software. The Stuxnet infection in 2010 led to an increase in cyber-attacks on U.S. assets. Since then, Iran has been devoting resources to developing its own cyber capabilities and organizations, some of which are part of the military and government, while others function

more freely. Some organizations focus on defensive skills and may collaborate with military groups engaged in offensive operations.

Iran has a history of using substitutes, including isolated attackers, private sector contractors, and quasi-governmental groups, to carry out cyber activities. By using partners, Iran can prevent attacks from worsening by maintaining plausible deniability. However, signs within the system's code indicate that Iran tries to claim attacks against foreign targets as proof of its capability. Iran has been engaged in cyber warfare since the 1990s, with the Iranian Cyber Army being responsible for some of the country's most damaging attacks. In 2009, DDoS attacks and online defacement targeted news organizations and websites connected to Western sponsored anti-Islamic revolution groups. In 2012-2013, Iranian hacker groups targeted 46 significant American financial organizations, such as J.P. Morgan, Chase, Wells Fargo, and American Express. Iranian cyber activities were primarily focused on the 2015 nuclear accord, with plans to attack European and American power grids, water treatment facilities, transportation networks, and banking institutions (“The Iranian Cyber Threat,” n.d.). Given how important cyber-attacks are to Iran's national security, the securitization and cyber-realism theory may foster insightful analysis of the country's defence tactics.

Iran’s Defensive Action against Cyber Attacks

Iran's government allocated $1 billion in July 2011 to enhance its cyber capabilities by acquiring new technologies and hiring cyber specialists. The country also established domestic organizations to manage cyberspace matters. In March 2012, the Supreme Council on Cyberspace was established, bringing all cyberspace agencies under one administrative authority (“The Iranian Cyber Threat,” nod). The council, comprising high-ranking Iranian officials, establishes Iran's internet policies and strategies. The Cyber Defence Command, under the Passive Defence Organisation, is the primary Iranian body responsible for cyber defense. It is governed by a committee led by the chief of staff of Iran's Armed Forces. The Passive Defence Organisation is responsible for coordinating government actions to prevent harm to sensitive locations and infrastructures, respond non-kinetically to military assaults. In response to the Stuxnet attack, the Cyber Defence Command was created in November 2010 to develop defensive cyber policy and minimize harm caused by cyber-attacks directed at Iran (“The Iranian Cyber Threat,” n.d.). Iran views cyber-attacks as existential dangers that are addressed by defensive measures.

Conclusion / Recommendations

Keeping in view the serious cyber-threats to its national security Iran is trying to become a one of the leading countries in cyber-technology and AI. In January 2022, Shahram Moein, head of the innovation and development centre of artificial intelligence at the Research Institute of Information and Communication Technology, emphasised, “Iran will be placed among the top 10 countries in artificial intelligence (AI) by 2032 based on the national document on artificial intelligence strategy.”(Tehran Times, February 27, 2024).

Cyber security is a critical concern for Iranians, especially as the internet becomes increasingly connected. The high frequency of malware, phishing attacks, and online surveillance pose significant threats to Iranian users and state institutions. To protect against these issues, it is essential to keep operating systems and anti-virus programs updated, avoid suspicious sites, use firewalls, and enable automatic updates. Iranian web users are also at risk from online surveillance, which can be circumvented by using virtual private networks (VPNs) or other encryption technologies. However, these tools may be unlawful and subject to government surveillance. Iranian consumers also have concerns about data privacy, which can be protected through two-factor authentication and unique passwords.

A balanced strategy involving organizational, technical, and strategic measures is advocated to strengthen Iran's cyber security measures against cyber-attacks. This includes investments in knowledge security measures, choosing a national framework, encouraging cooperation between public and private sectors, creating an efficient crisis management plan, purchasing advanced surveillance and mitigation tools, conducting frequent security audits, enhancing infrastructure security, facilitating safe international cooperation, creating online privacy staff tactics, and implementing stringent cybercrime laws (“Iran Cyber Threat Overview and Advisories | CISA,” n.d.).

By 2024, the digital environment will undergo significant transformation due to technologically advanced cyber threats. Artificial intelligence (AI) and machine learning (ML) are expected to play a larger role in cyber security, with improvements in IoT security protocols, block chain technology, and quantum technologies impacting cyber security. Quantum-resistant encryption methods, or post-quantum cryptography, are needed to address the potential for cracking established encryption techniques like RSA and ECC. In 2024, mobile security will become

crucial, with products like Splashtop offering secure access. Educational institutions and businesses are expanding cyber security curriculums and training programs to fill the skill gaps in cyber security (Morgan, 2022).

References

Analysis of the Iranian cyber-attack landscape. (2021, September 14). Retrieved from https://www.ironnet.com/blog/iranian-cyber-attack-updates

Artificial intelligence in cybersecurity: pros and cons. (n.d.). Retrieved from https://servreality.com/blog/artificial-intelligence-in-cybersecurity-pros-and-cons/

BBC News. (2012, April 22). Iran "building copy of captured US drone" RQ-170 Sentinel. Retrieved from https://www.bbc.co.uk/news/world-middle-east-17805201

Bencsáth, B., Pék, G., Buttyán, L., & Felegyhazi, M. (2011). Duqu: A Stuxnet-like malware found in the wild, Retrievedfrom: https://www.researchgate.net/publication/224963354_Duqu_A_Stuxnet-like_malware_found_in_the_wild

Codecademy. (n.d.). The evolution of cybersecurity, Retrieved from https://www.codecademy.com/article/evolution-of-cybersecurity

Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. (n.d.). Retrieved from https://icdt.osu.edu/countdown-zero-day-stuxnet-and-launch-worlds-first-digital-weapon

David E. Sanger. (2012). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. Retrieved from https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Enhancing Iran's cybersecurity: strategic measures and challenges. (2024, April 28). [Slide show]. Retrieved from https://www.slideshare.net/slideshow/enhancing-irans-cybersecurity-strategic-measures-and-challenges/267609533

Eroukhmanoff, C. (2020b, May 7). Securitisation Theory: An Introduction. Retrieved from https://www.e-ir.info/2018/01/14/securitisation-theory-an-introduction/#:~:text=According%20to%20securitisation%20theory%2C%20political,the%20issue%20'beyond%20politics'.

Essay on Cyber Technology - 1207 words | www2.bartleby.com. (n.d.). Retrieved from https://www2.bartleby.com/essay/Essay-On-Cyber-Technology-FCCJJFRJ9ER#google_vignette

Figueroa, W. (2023, February 16). China and Iran since the 25-Year Agreement: The limits of cooperation. *The Diplomat*. Retrieved from https://thediplomat.com/2022/01/china-and-iran-since-the-25-year-agreement-the-limits-of-cooperation/

Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. Retrieved from https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Ifmat, I. (2019, August 1). Part 3 - Iran's Threat to Cyber security. Retrieved from https://www.ifmat.org/04/26/iran-threat-cybersecurity/

Institute for Political and International Studies. (n.d.-b). Cyber-Threats and Cyber-Attacks against Iran. Retrieved from https://www.ipis.ir/en/subjectview/687242/cyber-threats-and-cyber-attacks-against-iran

Iran Cyber Threat Overview and Advisories | CISA. (n.d.). Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran#:~:text=Nation%2DState%20Cyber%20Actors,-China%20Cyber%20Threat&text=The%20Office%20of%20the%20Director,and%20allied%20networks%20and%20data.

Iran's cyber threat. (n.d.).

Retrieved from https://books.google.com/books/about/Iran_s_Cyber_Threat.html?id=w_dvuwEACAAJ

Jammal, A. F. (2023, October 4). Securitizing Iran's nuclear program: Unraveling Middle East power shifts. Retrieved from https://www.linkedin.com/pulse/securitizing-irans-nuclear-program-unraveling-middle-east-jammal

Jazeera, A. (2021, February 11). Iranian nuclear scientist killed by Israeli automated gun: Report. *Al Jazeera*. Retrieved from https://www.aljazeera.com/news/2021/2/11/iranian-nuclear-scientist-killed-by-israeli-automated-gun-report

Jnguyen. (2023, August 28). What is Cyber Security? The Different Types of Cybersecurity. Retrieved from https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/

Kamiński, M. A. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. *Security and Defence Quarterly*, *29*(2), 63–71. https://doi.org/10.35467/sdq/121974

Lee, D. (2012, May 28). Flame: Massive cyber-attack discovered, researchers say. Retrieved from https://www.bbc.com/news/technology-18238326

Lester, S. (2023, August 4). MYTH vs. FACT: Technology in Iran — American Iranian Council. Retrieved from http://www.us-iran.org/resources/technology

MacAskill, E. (2017, July 15). US drones hacked by Iraqi insurgents. *The Guardian*. Retrieved from https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked

Marcio Rocha and Daniel Farias Da Fonseca. (2019). The Cyber Issue and Realist Thinking. *The Cyber Issue in Realist Thinking*, 517–543.

Retrieved from https://portaldeperiodicos.marinha.mil.br/index.php/revistadaegn/article/download/4345/4730/#:~:text=THE%20CYBER%20ISSUE%20IN%20REALIST%20THINKING&text=The%20possibility%20of%20a%20state,influence%20the%20behavior%20of%20countries.

Michali. (2023, August 28). Biggest cyber security challenges in 2023. Retrieved from https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2023/

Morgan, J. (2022, September 29). 12 tips for mitigating Cyber Risk | JPMorgan Chase. Retrieved from https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk

Pfneisl, M. (2023, December 4). Triple Axis: Iran's Relations with Russia and China. Retrieved from https://vcdnp.org/triple-axis-irans-relations-with-russia-and-china/

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies/˜the œJournal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Roberts, I. (2024, March 8). Disadvantages with technology in cybersecurity. Retrieved from https://cybertheory.io/disadvantages-with-technology-in-cybersecurity/

Rodriguez-Hernandez, S. M., & Velásquez, N. (2021). Mexico and cybersecurity. In *Routledge eBooks* (pp. 484–493). https://doi.org/10.4324/9780429399718-41

Saxena, A. (2024, April 15). Importance of cyber security: Benefits and Disadvantages. Retrieved from https://sprinto.com/blog/importance-of-cyber-security/#Importance_of_cyber_security

Smith, T. (2023, November 19). The Global Landscape of AI Development: China, Russia, and Iran's Strategies and Impacts. Retrieved from https://www.concentric.io/blog/the-global-landscape-of-ai-development-china-russia-and-irans-strategies-and-impacts#:~:text=the%20Ukraine%20war.-,Iran,the%20AI%20market%20by%202032

Tariq, M. (2024, June 3). Israel and its alleged attacks on Iran: From drone strikes to cyberattacks. Retrieved from https://www.paradigmshift.com.pk/attacks-on-iran/

Tehran Times, (2022, January 30), "*Iran plans to become a leading country in AI"*, Retrieved from https://www.tehrantimes.com/news/469628/Iran-plans-to-become-a-leading-country-in-AI

Tehran Times, (February 27, 2024), *"Iran tops Islamic nations for AI documents",* Retrieved from *https://www.tehrantimes.com/news/495440/Iran-tops-Islamic-nations-for-AI-documents*

The Iranian Cyber Threat. (n.d.). *United Against Nuclear Iran*. Retrieved from https://www.unitedagainstnucleariran.com/iranian-cyber-threat-introduction

Trung Tran. (2022, November 15). A Glimpse of AI in Cybersecurity: Its Applications, Benefits & Also Drawbacks. Retrieved from https://www.orientsoftware.com/blog/ai-in-cybersecurity/

What is cybersecurity? (2024, February 22). Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html