International Journal of Political Science
ISSN: 2228-6217
Vol 14, No 3, Sep 2024, (pp.171-189)

A Study of Israeli Cyber Terrorism against the Islamic Republic of Iran with Emphasis on the Theory of the Network Society

Vahid Farid [1], Mohammad Reza Ghaedi[2*], Roohullah Ghasemian[3]

[1] Department of International Relations, Kish International Branch, Islamic Azad University, Kish, Iran
[2*] Department of Political Science, Shiraz Branch, Islamic Azad University, Shiraz, Iran
[3] Department of Political Science, Central Tehran Branch, Islamic Azad University, Tehran, Iran

Received: 10 Jan 2024 ; Accepted: 25 Sep 2024

Abstract

The Zionist regime is among the first states to institutionalize the importance of cyberspace within its national security doctrine, transforming it into an instrument for advancing its terrorist, military, security, and intelligence objectives. Given this regime's geopolitical constraints, prioritizing cyber capabilities as a form of asymmetric power has become an integral component of Tel Aviv's overarching security strategy. The regime's cyber-terrorist operations—particularly after the Stuxnet attack in 2010—entered a new phase in which cyberspace evolved into a domain for hybrid warfare, intelligence operations, and targeted attacks against Iran's critical infrastructure. Relying on existing evidence and documentation, this article examines examples of cyber-terrorist attacks attributed to Israel against Iran and analyzes the evolution of the regime's operational approaches over time. Accordingly, this study draws on network society theory to answer the central question: What is the role of cyberspace in the security dynamics between Iran and Israel, and what function does it serve in shaping the regional balance of power? The analysis indicates that Israel seeks to shift the arena of competition from the military domain to the social and perceptual spheres. This approach reflects the evolution of the doctrine of "deterrence through disruption" in the regime's cyber policy aimed at influencing Iran's societal security.

Keywords: Cyber terrorism, Network Society, Islamic Republic of Iran, Zionist Regime, Israel, National Security

[*]Corresponding Author's Email: M.Ghaedi@iau.ac.ir

Introduction

The emergence and expansion of cyberspace as the fifth dimension of national power—alongside land, air, sea, and space—has compelled states to design and implement new strategies in the cyber domain to preserve national security and maintain deterrence. The Zionist regime is among the first states to institutionalize the significance of cyberspace within its national security doctrine, transforming it into an instrument for advancing military, security, and intelligence objectives. Given this regime's geopolitical constraints and security vulnerabilities, an emphasis on cyber capabilities as a form of asymmetric power has become an inseparable component of Tel Aviv's overarching security strategy.

Cyber competition between Iran and the Zionist regime, especially after the 2010 Stuxnet cyber-attack, entered a new phase in which cyberspace evolved into an arena for hybrid warfare, intelligence operations, and targeted attacks against the critical infrastructure of both sides. Drawing upon existing evidence and documentation, this article explains the various dimensions of this competition, particularly by examining prominent examples of cyber-attacks attributed to the Zionist regime against Iran and analyzing the evolution of the regime's operational approaches over time. This evolution reflects a shift from complex, long-term attacks to short-term operations, followed by a return to hybrid patterns with an increased focus on social security in Iran.

1) Literature Review

Mirzaei and Ghoreishi (2024) in their article "Cyber Trojan Horses in Asia: An Analysis of the Israel–Iran Confrontation After the Stuxnet Attack" argue that the nuclear competition, initially Eurocentric, gradually shifted to Asia, where the presence of states such as India, Pakistan, North Korea, and Israel resulted in two-thirds of the world's nuclear powers concentrating in this region. Strengths of this study include its descriptive-analytical approach and its effective linkage between nuclear and cyber issues within the framework of regional security.

Amirli and Saqafi (2022), in their article "A Conceptual Model for Managing Threats Arising from Cyber terrorism," argue that the rapid expansion of cyberspace and the migration of a significant portion of citizens' and businesses' daily activities to this environment have created new opportunities for criminal and cyber terrorist activities. They note that many states, including the Islamic Republic of Iran, have identified this threat as a top security priority. Strengths of the study include its comprehensive conceptual model, derived from library-based data and expert opinions, which makes it both practical and strategic. Its main weakness lies in limiting validation to expert opinions rather than examining real statistical data, which could have enhanced its generalizability and operational credibility.

Hosseini and Jedari (2021), in their article "Examining the Effects of Cyber Threats and Attacks on the National Security of the Islamic Republic of Iran," emphasize that cyber threats and attacks, as a form of modern weaponry, can transform the conduct of contemporary warfare by both state and non-state actors. Notable strengths of this research include its comprehensive explanation of the impacts of cyber threats on national security and its attention to the role of non-state actors.

In the English-language literature, several studies also address this domain.

Epps (2021), in the article "Offensive Cyber Operations Reshaping the Modern Battle space," argues that contemporary states are increasingly using offensive cyber capabilities to influence the decisions and actions of their rivals, and that such operations play a central role in shaping and executing military planning. The article demonstrates that attacks on critical infrastructures—such as electricity, water, and national defense—represent concrete examples of the tangible impacts of offensive cyber operations. These actions, supported by information systems and enhanced intelligence-service capabilities, facilitate the emergence of overt, direct cyber warfare. Strengths of this study include its emphasis on the multilayered dimensions of cyber operations and its explanation of their role in contemporary military transformations. Its weakness, however, is its generality and the lack of in-depth case studies that could have enriched the research's analytical aspects.

Comiskey (2020), in the article "Operation Olympic Games: Cyber Sabotage as a Tool of the U.S. Intelligence Community to Disrupt Iran's Nuclear Program," explains that U.S. cyber activities against the Islamic Republic of Iran occurred through a covert campaign codenamed "Olympic Games," which began in 2006 during George W. Bush's presidency and focused primarily on disrupting Iran's nuclear capabilities. The findings indicate that large-scale cyber-attacks—such as the Stuxnet attack on Iran's nuclear facilities—are feasible only when powerful states equipped with advanced intelligence capabilities, diverse resources, and sophisticated cyber tools are involved. This demonstrates that cyber sabotage can be an effective tool for damaging the critical infrastructure of targeted states. Strengths of this research include its comprehensive analysis of the technical, security, and political aspects of the operation, as well as its examination of U.S.-Israeli cooperation. Its limitation lies in its focus on a single operation and its insufficient discussion of the long-term implications for Iran's national and human security.

Slayton (2020), in the article "The Future of Warfare: Israel's Cyber Posture Toward Iran," argues that the digital revolution has transformed the nature of conflict, compelling states—particularly those facing persistent military and security threats—to reassess their defensive strategies in light of technological advancements. A significant strength of this study is its exploration of the connection between national policymaking and Israel's cyber capacity-building, which highlights the multidimensional aspects of cyber power. Its weakness stems from an inadequate examination of operational features of the Iran-Israel cyber confrontation and the absence of a comprehensive comparative analysis of the cyber capabilities of both sides, which could have provided a clearer picture of the regional cyber balance.

2) Research Method

The present study employs a descriptive-analytical method and aims to identify and analyze the effects of the Zionist regime's cyber terrorism on the nuclear program and national security of the Islamic Republic of Iran during the period from 2003 to 2022. This method enables the researcher to examine the existing situation accurately and analyze its relationships and consequences without manipulating variables. Given the complex and multidimensional nature of the research topic—which includes technical, political, security, and social elements—the descriptive-analytical approach can provide a comprehensive and systematic picture of the trends and impacts of cyber terrorism.

3) Theoretical Foundations of the Research

3-1. the Theory of the Information and Communication Technology Revolution and the Network Society

With the beginning of the third millennium, profound transformations have emerged in the foundations of human social life. The core and essence of this transformation is what Manuel Castells terms the "information technology revolution." Once information technology became widespread, it experienced explosive growth and was adopted by diverse cultures and organizations for various purposes, becoming a source of new technological innovations. Electronic communication eventually transformed the entire world into a network, the control of which fell into the hands of a group of cosmopolitan elites. At the same time, the rest lost their control over their lives and environment (Qazi-zadeh, 2011, p. 38).

Among all the revolutions of the twentieth century, none has had an impact as enduring as the information and communication technology revolution. The boundaries that once separated human beings based on geographical, political, social, economic, and cultural characteristics have now disappeared. New technologies show no regard for the borders of authority and sovereignty (Bayat, 2006, p. 11).

A defining feature of the information technology revolution is not merely the centrality of knowledge and information, but the application of knowledge and information to produce knowledge and process information through an increasingly reinforcing feedback cycle between innovation and its applications (Castells, 2001, p. 61). Unlike earlier technological revolutions, which initially occurred within a limited number of societies and only gradually spread to others over many years, new information technologies expanded across the globe in less than two decades. Castells considers this a defining characteristic of the technological revolution, meaning that the direct use of the technologies it generates facilitates its further expansion and thus connects the world through information technology (Rosenau & Singh, 2002, p. 14).

3-2. Manuel Castells' Network Society

Terms such as informational society, network society, cyber society, digital society, silicon civilization, and perhaps other similar expressions have been used over recent decades to

understand the political, social, economic, and cultural dimensions of life and to illustrate the latest manifestations of modern human existence. In this regard, numerous scholars in the humanities—including Daniel Bell with his theory of the "information society as post-industrialism," Anthony Giddens with the theory of "information, the nation-state, and surveillance," Herbert Schiller with the theory of "information and advanced capitalist prestructures," Jürgen Habermas with the theory of "the management and manipulation of information and the destruction of the public sphere," Manuel Castells with the theory of the "network society," as well as other thinkers such as Jean Baudrillard and Jean-François Lyotard—have described "information and communication technologies" as the defining feature of the contemporary world (Vister, 2004, pp. 25-28).

The term "network society" first entered academic discourse in 1997, introduced by Manuel Castells. Castells is among the sociologists who have conceptualized the transformations of modern society derived from the expansion of information technologies—such as mobile communication, the Internet, and mass communication networks—and who have offered an independent and relatively comprehensive methodological framework. Some regard Castells as the most influential global and exclusive theorist of the information age, unmatched by any other scholar to date (Mazarr, 2002, p. 5).

Castells' theoretical foundation rests on the concept of the network society. According to Castells, the global network society is one in which social structures are formed around networks activated by information, communication, and digitally processed technologies based on microelectronics. In this society, networks dominate activities, and individuals who are considered "external" or "outside" these networks, in turn, lead to the decline of local networks (Castells, 2014, p. 83).

According to Castells, the core of the network society is information technology, which significantly facilitates the spread of this process (Zolghadr & Ghasemzadeh Araki, 2012, p. 175). The rapid expansion of information and communication technologies has transformed human life in its political, security, economic, and social dimensions, giving rise to the network society. This transformation has even been labeled the "third industrial revolution" (Bell, 2007, p. 59).

3-3. Characteristics of the Network Society

In the global network society, all human affairs—such as values, identity, the division of labor, the concepts of time and space, and even power—become dependent on networks. It is the objectives, characteristics, structures, and programs of the networks that define human affairs. In this society, value is determined by the network's hierarchical structure, shaped by actors operating within it. Labor is also characterized by global networks of production, distribution, and resources into two groups: self-programming labor and generic labor.

Networks herald the dominance of the "space of flows" over the "space of places," giving rise to a new spatial form of society. Furthermore, the culture of the network society becomes a culture of communication protocols; the nation-state is transformed; the network state emerges; and ultimately, power in the network society is held by those who control the communicative capacities among networks and the groups within them (Divsalar, 2014, p. 94).

The internal dynamics of the network society continuously reshape the relations within these networks. Following the logic of networking, they constantly transcend existing boundaries and move towards establishing more expansive institutions. Some manifestations of this network logic include: the fluid and ever-evolving morphology of social forms and the architecture of network structures; the rapid and large-scale movement of capital within networks that renders local monitoring and control ineffective; the increasing individualization of human resources within networks that transform them into replaceable identities; the activation of strategically connected regions and individuals, while less significant areas and disconnected individuals become inactive.

However, perhaps the most crucial aspect of the network's internal logic is that it creates conditions under which many phenomena that possess a singular nature in a conventional, non-network environment acquire a paradoxical dual character. For example, within the network society, nation-states—which under traditional circumstances represent national will, sovereignty, and territorial integrity—are, on the one hand, weakened to the extent that they lose the ability to control information or capital within their borders, and on the other hand, become capable of generating major ethnic and racial crises (Castells, 2001, pp. 18-19).

4) Cyberspace and Emerging Security Challenges in Inter-State Relations

With the rapid expansion of information and communication technologies and the widespread penetration of the Internet into individual, social, and organizational life, cyberspace has become one of the primary arenas of competition and power at both national and international levels. This transformation has not only enabled broad access to and exchange of information but has also fundamentally reshaped the structure of control and security relations. The emergence of cyber power is a multidimensional concept that encompasses the ability of states and non-state actors to exploit the digital domain for political, economic, military, and social objectives; while simultaneously generating new threats whose nature and mechanisms differ significantly from traditional security challenges.

Cyberspace refers to a complex set of human interactions and communications conducted through computers and digital technologies, unconstrained by specific physical locations or geographical borders. This domain extends beyond the World Wide Web or the Internet alone, encompassing a wide array of digital tools, systems, and telecommunications infrastructures that enable reciprocal and interactive communication among individuals. In this information-driven environment, greater attention is directed towards content and the manner in which data is exchanged, as individuals engage with one another directly and collaboratively rather than merely serving as passive senders or receivers of information (Zafari et al., 2021, p. 51).

Cyberspace—an innovative product of the digital world and electronic communication—

not only provides unprecedented opportunities for communication, cultural exchange, and the expansion of social interactions, but also offers diverse capabilities for cultural penetration, soft-power projection, and even the conduct of psychological operations. These characteristics have made cyberspace not only an arena for advancing economic, educational, and social goals, but also a critical space for global-scale cultural and security competition. Consequently, its strategic significance in national and international policymaking has increasingly been emphasized (Gharib, 2021, p. 114).

The concept of cyber power may be examined within the same analytical framework used for sea power, air power, land power, and even space power, as such comparisons help clarify its role within contemporary security and military orders. Daniel T. Kuehl defines cyber power as the capability and capacity to use cyberspace to generate strategic advantages and influence events across the entire operational environment—including land, sea, air, space, and cyberspace itself. He stresses that such influence can be exerted through all instruments of national power, including diplomacy, information, military force, and economic capacity (Kuehl, 2009, p. 29). Similarly, John B. Sheldon underscores that cyberspace can exert significant influence across all domains simultaneously, a feature that distinguishes it from other realms of power (Sheldon, 2012, p. 11).

Joseph Nye, on the other hand, argues that cyber power depends primarily on the resources and infrastructure that shape this domain's unique characteristics and differentiate it from others. He defines power as the ability to achieve desired outcomes through the purposeful use of available tools and capabilities within cyberspace and other arenas, such that cyber power constitutes not merely a technological capacity but a multidimensional strategic component in global politics and security (Nye, 2011, p. 8). Consequently, cyber power, as a central instrument in contemporary strategic competition, can exert broad, simultaneous, and multi-layered influence across all domains of power, and its role in shaping operational environments and strategic decision-making has become increasingly prominent.

5) The Position of Cyberspace in Israel's National Security Strategy

For Israel, cyberspace has from the outset been not merely a technical domain but a strategic arena encompassing both the defense of critical infrastructure and the instrumentalization of soft and hard power. In other words, Israeli policymakers regard cyberspace as both an essential component for ensuring the continuous functioning of the state and a platform for advancing military and intelligence interests. This dual function led to the creation of a specialized organizational and legal structure that integrates defensive, regulatory, and developmental tasks while placing cooperation among military, intelligence, governmental, academic, and private-sector institutions at its core. The result is that cyberspace has ceased to be a purely technical field and has instead become a policymaking entry point influencing national security decisions and diplomacy (Frei, 2020, p. 5).

Within this strategic framework, achieving "comprehensive information dominance" has been emphasized as a key factor for success in the rapidly evolving security environment of the Middle East and as a prerequisite for understanding changes and responding to threats quickly. From the perspective of Israeli

decision-makers, such intelligence dominance constitutes the fundamental basis for maintaining military superiority and ensuring the regime's security against regional adversaries, because without it, even the most advanced military and defensive capabilities would lack a practical and deterrent function.

In this context, Israel's deliberate effort to become a "global cyber power" is part of its overarching national security strategy, rooted in the regime's existential nature and security-centric structure. Founded through occupation and facing ongoing legitimacy crises, Israel has consistently experienced chronic insecurity; therefore, security considerations form the core of its political, military, and technological decision-making. From this viewpoint, Israeli leaders identified cyberspace—earlier than many major global powers—not merely as a communication and technological domain but as a new security and warfare environment, and subsequently developed comprehensive plans for active, defensive, and offensive engagement within it.

This approach is explicitly reflected in Israeli military doctrine, which stresses the simultaneous enhancement of both offensive and defensive cyber capabilities. Accordingly, the establishment of organized structures such as a "cyber army" under the direct supervision of the Chief of General Staff has been prioritized to enable the regime to maintain integrated surveillance of cyberspace, identify threats, and conduct targeted cyber operations. Alongside these initiatives, significant attention has been directed towards enhancing Israel's technical, scientific, and technological capabilities, ensuring that the state maintains its technological superiority, readiness, and operational maneuverability in future cyber conflicts (Torabi, 2016, pp. 164-165).

From an operational standpoint, Israel has worked simultaneously along three principal axes: robustness, resilience/incident response, and the cultivation of deterrent and offensive capabilities against both state and non-state actors. This three-layered approach ensures that military and intelligence bodies—particularly specialized units such as Unit 8200—can act both as supervisors and defenders of infrastructure and as holders of offensive and deterrent capabilities. This fusion of defense and offense within Israel's national policymaking has made cyberspace an inseparable component of Israel's military posture and deterrence calculations (IISS, 2021, p. 69).

Israel's national strategy explicitly identifies investment in national innovation structures—research and development centers, clusters such as "Cyber Spark," and mechanisms for transferring military knowledge to industry—as a geostrategic necessity. This military-civilian synergy has not only accelerated industrial and commercial growth in the cyber sector but also sustains and renews operational and cyber-intelligence capacities. Thus, cyberspace in Israel's national security strategy is considered both a defensive tool and a driver of economic and technological empowerment (Matania & Yoffe, 2022, p. 103).

In the 2019 World Economic Forum, Netanyahu also claimed that Israel intends to become a "cyber greenhouse." He encouraged

states to invest in Israeli cyber security products and to cooperate with the regime in this domain. The analogy implies that, just as a greenhouse provides the conditions for plant growth, Israel seeks to foster cyber security growth in other states. Whether Israel has truly reached a position that would allow it to call itself the global leader in all dimensions of cyber power remains a matter of debate. Nevertheless, Israel presents itself as a significant cyber defense power. Cyber espionage is another domain in which Israel exerts considerable effort. Unit 8200—as an operational entity—and institutions such as Ben-Gurion University and Be'er Sheva—as centers of research and innovation—play crucial roles in enabling the regime to achieve high levels of cyber-espionage capability (Zanjani, 2019, p. 154).

Unit 8200 is recognized as one of the key institutions involved in cyber security and electronic operations within the Israeli regime. Although its official mission is often framed in a defensive context, in practice, the unit does not hesitate to employ offensive and preemptive measures to achieve its strategic objectives. The operational core of Unit 8200 consists of its signals intelligence (SIGINT) division, which possesses deep expertise in electronic warfare, decryption, and the analysis of communications signals. Its activities include analyzing publicly available information as well as employing both human operators and artificial-intelligence-based systems to process data and extract patterns.

Unit 8200 is responsible for intercepting, recording, decrypting, and interpreting a vast range of communications. It has established a relatively global structure for information collection and exchange through a network of SIGINT bases and listening stations. Within this framework, the Urim base—with its powerful antennas and receivers—provides the capability to monitor telephone calls, electronic messages, and other communications flows across the region and far beyond—from the Middle East to Europe, Asia, and Africa. Urim also serves as a critical infrastructure site for monitoring undersea cables and maritime communication traffic, demonstrating the unit's signal intelligence capabilities that extend well beyond geographical boundaries.

In addition to defensive operations, Unit 8200 conducts offensive cyber operations, leveraging a variety of tools and covert listening posts to enhance its capabilities. These posts include listening stations located in Israeli embassies abroad, as well as units stationed within the occupied Palestinian territories. At the same time, its use of Gulfstream aircraft equipped with electronic surveillance systems indicates the integration of air and ground platforms in its data-gathering methods. Analytically, this combination of capabilities reveals the hybrid and dual nature of Unit 8200. This institution simultaneously claims to defend national cyber security while actively engaging in electronic espionage and preemptive operations. Such a configuration raises serious questions regarding legal boundaries, international accountability, and the geopolitical implications of deploying signal-intelligence capabilities for intrusion and influence in the political, economic, and military domains of other states—issues that deserve careful attention in legal and security analyses concerning similar units (Sean, 2019, p. 8).

Overall, it can be stated that Israel has embraced cyberspace as one of the main pillars of its national security strategy, pursuing "absolute intelligence dominance" and the attainment of superior cyber power as prerequisites for preserving its military superiority, deterrence, and national security. This approach

has led Israeli policymakers and commanders to view cyberspace not merely as a technological domain, but as a battlefield and a strategic arena of influence. At the same time, they have invested in strengthening defensive and offensive cyber capabilities, creating organized institutions such as a "cyber army," and relying on specialized electronic intelligence and signal-collection units (such as Unit 8200). Beyond military structures, supportive policies for research and education in universities and the industrial growth of cybersecurity companies (both domestically and through registrations in the United States) constitute part of a broader strategy to create a "cyber greenhouse" and commercialize national cyber capabilities. The goal is both to develop defensive and offensive technologies and to establish a global market for Israeli cyber products. In practice, this combination of a trained workforce, technological institutions, and intelligence-gathering networks enables offensive and disruptive capabilities targeting critical infrastructure and helps preserve Israel's strategic superiority.

6. Cyber Competition Between the Islamic Republic of Iran and the Zionist Regime

The interconnectedness of today's world in the era of communications and information technology—despite creating unprecedented opportunities—has also generated significant concerns. One primary concern is human security, which is severely threatened by cyberattacks and espionage. Thousands of cyberattacks occur worldwide every day, making it difficult to distinguish between serious and less severe attacks (Kramer, 2009, p. 15). In this context, the role of the internet in the security of the Islamic Republic of Iran and the Zionist regime can be assessed in three specific domains.

First domain: wars arising from the confrontation between the two states, referred to as Cyber War and similar terms. In this type of conflict, the adversary's computer networks are attacked and sabotaged to weaken and disrupt the target state's capabilities—what is commonly described today as a Hard Threat (Kovačič & Boni, 2014, p. 5).

Second domain: threats whose origins are not necessarily foreign governments, but which fall within the realm of internal security, including human security. Examples include computer espionage, hacking websites, eavesdropping on citizens' communications, and intrusions into personal digital spaces. These are categorized as Half-Hard Threats.

Third domain: threats aimed at altering identities, beliefs, attitudes, and values within society to influence the governing system. These are referred to as Soft Threats (Anaami, 2008, pp. 39-40).

For nearly two decades, Iran and the Zionist regime have been engaged in a long-term, multifaceted cyber competition characterized by a combination of cyber espionage, disruptive/destructive operations, and information-infiltration campaigns. Within this framework, both sides employ covert and proxy-based tactics to maximize impact while

minimizing cost and direct accountability. Because of its technological concentration and advanced intelligence capabilities, Israel generally acts more offensively, conducting precisely targeted operations (including attempts to disrupt industrial systems or sensitive networks). Iran, by contrast, relies on a diverse set of state and semi-state actors and hacking groups to carry out disruptive, doxxing-oriented, and infiltration operations designed to increase political pressure and impose costs on Israeli targets. This dynamic not only reflects the technological implications of the rivalry but has also created new patterns of "below-threshold cost-imposition" in regional security policy (Microsoft, 2024, p. 2).

After the initial phase of basic skill-building, the cyber rivalry gradually evolved into a competition over capabilities and resilience. Each time one side develops new tools for intrusion or disruption, the other rapidly reallocates resources to protect critical infrastructure, strengthen detection and incident response, and develop adaptive deterrence capabilities. Technically, Iran's model includes a wide array of state-linked APT groups, social-engineering tactics, and targeting of OT/ICS systems. Israel's model—combining state intelligence resources with a strong private-sector tech ecosystem (cyber security firms and start-ups)—produces advanced offensive and defensive capabilities. This dynamic elevates competition not only operationally but also through rapid innovation and the transfer of knowledge and technology (Trellix, 2024, p. 7).

The strategic consequences of this rivalry are complex:

First, the likelihood of escalatory disruption increases—cyber-attacks can quickly escalate into military responses or diplomatic pressure. Second, political and legal costs for third parties and civilian infrastructure have risen, complicating questions of responsibility and the legitimacy of cyber operations.

Third, the Iran-Israel cyber rivalry creates replicable models for regional and extra-regional actors who may adopt or imitate these capabilities, thereby reshaping regional stability (CSIS, 2024, p. 3).

7. The Most Significant Cyber-attacks attributed to the Zionist Regime against Iran

In recent decades, globalization has not only transformed economic and political relations but also reshaped the structure and nature of international security. This transformation—particularly through the expansion of the digital and networked environment—has led to the emergence of new types of transnational and non-state threats that transcend traditional boundaries of power and security. In this context, the Islamic Republic of Iran, like many developing countries, has been exposed to a form of "technological insecurity." This means that cyber vulnerabilities have become a fundamental challenge to national security. Unlike classical military threats, which have a physical and identifiable nature, cyber threats are asymmetric, unpredictable, multilayered, and operate through platforms such as information networks, critical infrastructure, and digital communications.

Over the past two decades, as the internet has become widespread and computer technologies have penetrated all levels of society—from households to government institutions and economic enterprises—the potential capacity for cyber-attacks and malware dissemination has increased dramatically. The ease of computer use, user anonymity, and growing

dependence on communication networks have created a dangerous combination that has reduced state control over cyberspace while increasing the penetration capabilities of non-state actors. From this perspective, cyberspace has turned into a stage for geopolitical rivalry and soft warfare, where the destructive power of cyber operations can substitute for traditional military force.

In a 2015 report, the Russian company Kaspersky announced that Iran is the most infected country, with its computers and networks in the economic, diplomatic, research, academic, and telecommunications sectors targeted by intrusions and cyber-attacks using malware and viruses. Kaspersky did not explicitly name the countries responsible for these attacks. According to the company, after Iran, the highest levels of cyber infection were found in Russia, Pakistan, Afghanistan, China, Mali, Syria, Yemen, and Algeria (Passive Defense Organization of Iran, 2015, p. 15).

This section focuses on analyzing and explaining the most significant non-nuclear cyber-attacks attributed to the Zionist regime against the Islamic Republic of Iran—attacks that, over the past two decades, have targeted the country's critical infrastructure, including the industrial, energy, transportation, and public service sectors. The goal is to examine the technical, strategic, and political dimensions of these attacks and assess their implications for national security and the effectiveness of Iran's cyber policy-making system. Since the Zionist regime employs cyber tools as part of Hybrid Warfare to exert pressure and undermine Iran's internal capacities, this section seeks to analyze the patterns, objectives, and methods of these cyber operations. It should be noted that this chapter focuses exclusively on non-nuclear cyber-attacks, while a detailed examination of cyber-attacks and terrorist operations against Iran's nuclear facilities—as key examples of "cyber nuclear terrorism"—will be addressed comprehensively in the next chapter.

7-1. Cyber-attack on the Natanz Nuclear Facility through the Stuxnet Malware (2010)

The first documented, large-scale instance of using malware to damage infrastructure physically occurred in the 2010 attack on the control systems of the Natanz nuclear facility. On July 13, 2010, the VBA32 antivirus identified a virus named Stuxnet, which rapidly spread worldwide, especially in Iran. The Stuxnet malware was designed to infiltrate industrial control systems, particularly controllers that regulate the rotation of uranium-enrichment centrifuges. It was transferred through removable drives to a network that appeared to be isolated from the internet (Zetter, 2015, p. 5). The significance of this incident lies in the fact that, for the first time, cyber warfare moved beyond information intrusion and digital espionage into the realm of physical and operational destruction of critical national infrastructure. The discovery of this malware by security experts reshaped global perceptions of cyber threats and introduced the concept of "preemptive cyber warfare" into the vocabulary of international security.

The purpose of this virus was to disrupt companies and organizations that operate critical infrastructure, such as power plants. This malware spread by exploiting Windows security vulnerability and targeted systems running Siemens' WinCC SCADA software, which was designed for atomic centrifuges (Eskandari, 2011, p. 12). The attack turned off nearly 1,000 centrifuges and infected 30,000 computers. Iran was forced to take tens of thousands of computers offline. The Stuxnet attack represented a multinational approach to offensive cyber operations against Iran (Chomsky, 2020, pp. 64-70).

From a technical standpoint, Stuxnet demonstrated a level of complexity and cyber engineering unprecedented in any previously known operation. The malware exploited multiple zero-day vulnerabilities in operating systems and used valid digital certificates to masquerade as legitimate software, thereby bypassing detection mechanisms. Its core function involved rewriting the control programs of industrial systems and gradually altering the rotational speeds of centrifuges so that the machines would experience wear and failure without issuing any direct alerts. Simultaneously, the malware produced falsified data on engineers' screens, creating the impression that everything was functioning normally. This sophisticated synchronization between software and physical machinery indicated that Stuxnet's design was the product of coordinated efforts among specialists in hardware, industrial programming, and nuclear engineering (Fallière, 2011, p. 2).

7-2. Cyber-attack on the Telecommunication Company of Iran through the Duqu Malware (2011)

In April 2011, an advanced virus named Duqu was identified, which displayed remarkable structural and functional similarities to the well-known Stuxnet virus. Technical analyses revealed that large portions of Duqu's source code had been effectively rewritten or reused from the original Stuxnet code. In some segments, the two were nearly identical line by line. This technical resemblance led cyber security experts to refer to Duqu as "Stuxnet 2.0" or the "son of Stuxnet." After infiltrating computer systems, Duqu established communication with command-and-control servers and, through this channel, received new instructions and numerous malicious files. This feature made Duqu a dynamic, expandable tool capable of executing a range of cyber missions.

Moreover, if the infected system was connected to a network, the malware could map the entire network, identify vulnerabilities, and transmit the results to its command servers. Such capabilities indicate the purposeful and professional design of this malware for espionage and the collection of sensitive industrial and security-related information (Utinkova, 2021, pp. 26-27).

7-3. Cyber-attack on Iran's Oil Facilities through the Flame Malware (2012)

Flame is a complex, multifunctional, modular malware produced by a sophisticated team approximately two years after the emergence of Stuxnet, with the primary purpose of cyber espionage. It succeeded in infecting several of Iran's oil facilities. Reports indicate certain similarities between Flame and Stuxnet. According to the Iranian Information Technology Organization, Flame is among the most complex malware programs ever detected, equipped with extensive encryption mechanisms. Tests showed that 43 different antivirus programs could not identify it. Based on its

behavior, this virus was significantly more potent than Stuxnet (Constantin, 2015, p. 2).

The malware spread primarily across Middle Eastern countries, with Iran being among the most severely affected. Although Stuxnet had already amazed researchers with its technical sophistication, Flame surpassed it in complexity. As Alexander Gostev, a senior security expert at Kaspersky Lab explained: "It took us six months to analyze Stuxnet […]. But Flame is 20 times more complex. It may take ten years to understand everything fully. It can be described as a toolbox, meaning that it uses multiple different tools to achieve its objective." This is precisely what made Flame such a powerful tool for infecting computer systems, with its array of operations including "network traffic monitoring, screenshot capture, audio recording, keystroke logging, and more."

Another striking feature of Flame was its ability to turn an infected device into a type of "beacon," activating Bluetooth and scanning for nearby Bluetooth-enabled devices. Additionally, if the threat actor uploaded additional tools to the infected system, the malware's capabilities could expand. Flame also concealed its own traces; after transmitting stolen data, it deleted all associated files, erased itself, and wiped the disk. Overall, the primary function of this cyber-attack was the collection and transfer of data—in other words, cyber espionage. This operation caused extensive damage to the victims' computer systems (Utinkova, 2021, p. 26).

7-4. Theft of Sensitive Information through the Gauss Malware (2012)

Gauss was one of the most prominent data-oriented malware programs of 2012. By precisely targeting selected hosts and employing encrypted modules, it enabled the large-scale theft of sensitive data. Technical evidence and its deployment pattern indicate that Iran was one of the regional targets of this malware family, and that organizational networks, as well as communication and financial accounts associated with Iranian actors, were among the identified targets.

Gauss's modular architecture, its ability to infect removable media such as USB drives, and the presence of encrypted components that activate only on specific systems demonstrate a deliberate design for long-term infiltration and systematic data extraction. These characteristics—combined with network-related evidence and expert analyses—show that the objective of this malware went far beyond ordinary cybercriminal profit and was directed at state-linked actors and sensitive institutions in the region (Skingsley, 2023, p. 80).

Nevertheless, Gauss's most distinctive feature was his ability to steal banking information, affecting thousands of victims, most of whom were located in Iran, Lebanon, and Palestine. The purpose of this attack was likely to gather intelligence on Hezbollah's financial links with Iran (Bencsath et al., 2012).

7-5. Cyberattack on Shahid Rajaee Port in Southern Iran (2020)

On 9 May 2020, a large-scale cyberattack targeted the infrastructure of Shahid Rajaee Port in southern Iran, disrupting the control systems governing ship and truck movements and logistical operations. As a result, the port's activities were halted for several days. The objective of this type of operation was to damage critical nodes in the supply chain and cause operational disruption, even if temporarily. On May 15, 2020, Israel's Ministry of Defense announced that, from Iran's perspective, this incident was the third cyber operation since December 2019 that had led to port shutdowns. Such repeated attacks not only indicate the technical capabilities of the perpetrators but also confirm that cyber vulnerabilities exist within Iran's critical infrastructure, which the adversary exploits as a tool of pressure and deterrence (Siman & Even, 2020, p. 3).

Attributing cyber operations to a specific actor is often complex and requires independent technical analysis. Nevertheless, official Israeli statements and the tone of remarks by its officials suggest that this approach was designed within the framework of Israel's multidimensional pressure strategy. Naftali Bennett, the regime's Minister of Defense, stated on May 18, 2020: "The Iranian octopus sends its tentacles to claw at us from every direction... we must also intensify our political, economic, military, and technological pressure. This can be done." General Aviv Kochavi, Chief of Staff of the Israeli Army, declared on May 19, 2020, that "the Israeli military will continue to use various military tools and unique combat methods to harm the enemy" (Siman & Even, 2020, p. 4).

7-6. Cyberattack on Iran's Gas Stations (2021)

The large-scale cyberattack on Iran's innovative fuel system in October 2021—which caused thousands of gas stations across the country to fail—is considered one of the most sophisticated cyber operations against Iran's critical infrastructure. Technical analysis of the incident shows that the attackers infiltrated the software layer of the fuel distribution network, disrupting communication between point-of-sale terminals and the central server. This effectively halted subsidized payments and digital transactions. The attack not only revealed the vulnerabilities of operational and information technology systems in Iran's critical infrastructure but also demonstrated that cyber operations can cripple functionality without physical destruction, creating widespread social and psychological consequences at the national level.

The timing of the incident, coinciding with regional political tensions, strengthened speculation regarding Israel's role—especially since the attack pattern and the messages displayed on screens bore significant resemblance to previous operations attributed to groups affiliated with Tel Aviv (Reuters, 2021, p. 1).

Cyber security analysts believe that the primary objective of this operation was not merely technical disruption but rather to undermine the government's perceived competence and public trust in its ability to manage vital services. Within the framework of its "active cyber deterrence" strategy, Israel employs such operations to erode Iran's resilience. The attack demonstrated that even with network segmentation and claims of infrastructure independence, the software supply chain and human points of contact remain the most vulnerable links in national security (Wired, 2024, p. 5).

7-7. Cyberattack on Iran's Steel Industry (2022)

On June 27, 2022, the systems of three steel manufacturing companies in Isfahan, Khuzestan, and Hormozgan were targeted in cyber-attacks. Although hours after the incident, a cyber-group calling itself "Predatory Sparrow" released a video claiming responsibility for the attack—describing it as a response to the "regional actions of the Islamic Republic"—Iran attributed the attack to Israel and the United States (Euronews Persian, 27/06/2022).

The 2022 cyberattack on Iran's steel industry represents one of the most prominent examples of targeted cyber warfare against critical Iranian infrastructure, comparable in depth of penetration, technical complexity, and economic impact to previous attacks on the Natanz nuclear facilities. Initial assessments showed that the attackers gained unauthorized access to industrial control systems and monitoring platforms governing melting and casting lines, briefly disrupting process controls. As a result, several major complexes, including Khuzestan Steel and Mobarakeh Steel, faced temporary production shutdowns. Technical analyses indicated that the intrusion pathway operated through contractor accounts and intermediary management software, in which data encryption and remote control played key roles (Cyber scoop, 2022, p. 2).

This attack can be seen as part of Israel's strategic pattern of employing cyber operations with economic and symbolic consequences against Iran. The group known as Predatory Sparrow—which had also been linked to prior attacks on fuel distribution—claimed responsibility and reinforced the psychological and media dimension of the operation through the release of targeted images and messages. The aim of such actions is not only to disrupt industrial functionality but also to undermine the perceived managerial effectiveness of the Islamic Republic in safeguarding sensitive infrastructure (Wired, 2024, p. 5).

From a national security perspective, this attack reflects the transition of cyber warfare from information intrusion to destructive operations with direct implications for the economy and energy security. Furthermore, the semi-overt nature of the attack suggests that Israel is adopting a strategy of "overt cyber deterrence," using the display of technological power to raise the political cost of potential Iranian counterattacks. Under such circumstances, developing an industrial cyber-defense doctrine, enhancing threat-monitoring systems, and localizing industrial control software appear to be essential pillars for strengthening national resilience.

The cases, as mentioned earlier, represent only a small portion of the extensive scope of Israel's cyber warfare against the Islamic Republic of Iran. This ongoing but concealed conflict has unfolded over the past two decades across infrastructural, industrial, communication, petroleum, and even societal and media domains. Studies indicate that these attacks are not merely intended to disrupt technical systems but are designed to weaken Iran's deterrence capacity, discredit its technological capabilities, and influence public perception. In reality, Israel's cyber strategy towards Iran should be understood as part of its broader "hybrid deterrence" policy, which

integrates intelligence operations, digital sabotage, and cognitive warfare. The persistence and variety of cyber-attacks attributed to Israel demonstrate that the cyber confrontation between the two sides has surpassed episodic actions and has become a stable component of Iran's national security equation and strategic deterrence framework.

Conclusion

In recent decades, the expansion of cyberspace and the growing dependence of societies on digital infrastructure have fundamentally transformed the concepts of power and security in the international system. The emergence of modern information and communication technologies has not only altered patterns of interaction among states but also reshaped the global landscape. Still, it has also provided new tools for exercising power, causing disruption, and enforcing deterrence. In this context, the phenomenon of "cyber terrorism," as a novel form of transnational threat, has become a strategic instrument for regional and global powers to target their rivals' vital interests without engaging in conventional warfare. One of the most prominent manifestations of this trend is the cyber confrontation between the Israeli regime and the Islamic Republic of Iran, which, through destructive cyber-attacks—including malware such as Stuxnet—has created a new dimension of covert warfare. Such confrontations are not only technical and technological in nature but also have extensive political, security, and social ramifications, raising the question of how technological developments can challenge a country's national security from within.

Within this framework, the present study aims to examine the impact of Israeli cyber terrorism on the national security of the Islamic Republic of Iran, based on Manuel Castells' theory of the "Information Technology Revolution and Network Society." Employing this theoretical approach enabled the research to understand the networked and technological nature of power in the information age and to explain the security and social dimensions of cyber threats at both national and transnational levels. This approach offers a theoretical response to the reality that cyber threats cannot be analyzed solely within the framework of hardware security; social, psychological, and human factors also influence national security. Using a descriptive-analytical method and drawing on library data and qualitative content analysis, the research sought to examine, within Iran's territorial context, the interplay among technology, politics, and security from the perspective of Israeli cyber threats and attacks. The author's primary concern in this study is to gain a deeper understanding of the connection between technological power and national security in a context where the battlefield has shifted from physical domains to cyberspace, rendering Iranian human security a multidimensional and complex concept under cyber warfare.

The findings of this study indicate that advancements in information and communication technologies, particularly the expansion of the internet and the creation of cyberspace, have challenged traditional patterns of power and security, paving the way for a new type of conflict in international relations. In this context, the boundaries between war and peace, state and non-state actors, and physical and virtual spaces have become increasingly blurred. In the information age, power relies less on military superiority or material resources and more on control over data flows, communication networks, and technological

capacities. This fundamental shift has created a new concept of power and security, in which cyberspace is not merely an auxiliary tool but an independent arena for action, deterrence, and threat. From this transformation, cyber terrorism has emerged as a novel manifestation of transnational threats—a threat characterized by invisibility, anonymity of perpetrators, speed and breadth of impact, and low cost of action, making it an effective tool for both state and non-state actors. Among these actors, Israel stands out as one of the pioneering states leveraging cyberspace to advance its security and strategic objectives, converting technology into a tool of power and adopting an aggressive and hybrid approach towards regional competitors, particularly the Islamic Republic of Iran.

The results of this study demonstrate that security in the digital age is no longer solely a military or technical concept but has evolved into a combination of technological, human, social, and perceptual dimensions. From this perspective, the present research not only contributes to enhancing Iran's national security but also lays the foundation for developing an indigenous theoretical literature on cyber security and serves as a guide for policymakers, researchers, and future specialists in the field of digital security.

References

Anaami, S. (2008). "Soft threats: The U.S. strategic counter-pattern against Iran." Jomhoor Report (Presidential Research Center), 26–27, 3–42.

Bayat, M. (2006). Digital diplomacy: A study of contemporary diplomatic transformations. Tehran: Printing and Publishing Center, Ministry of Foreign Affairs.

Bell, D. (2007). Cyber culture theorists: Manuel Castells and Donna Hardaway. Rutledge.

Bencsath, B., Pek, G., Buttyan, L., & Felegyhazi, M. (2012). The cousins of Stuxnet: Duqu, Flame, and Gauss. Future Internet, 971–1003.

Castells, M. (2001). The Information age: Economy, society, and culture (The rise of the network society, Vol. 1) (A. Aligholian & A. Khakbaz, Trans.). Tehran: Tarh-e No.

Castells, M. (2014). Communication power (H. Basirian Jahromi, Trans.). Tehran: Research Institute for Culture, Art, and Communication.

Constantin, L. (2015). The Duqu spy group also targeted telecommunications companies. Retrieved from http://www.pcworld.co.nz/article/577233/duqu-spy-group-also-targeted-telecommunications-companies

Divsalar, A. R. (2014). "Communication power or information power: A

critique of Manuel Castells' network power theory." Book Review Quarterly: Information and Communication, 1(3–4), 91–110.

Eskandari, H. (2011). Cyber defense and computer security (1): General security in information technology. Tehran: Boston Hamid Publications.

Euronews Persian. (2022, June 27). "Cyberattack on Khuzestan Steel Company." Retrieved from: https://parsi.euronews.com/2022/06/27/cyber-attack-on-khuzestan-steel-company-a-hacker-group-claimed-responsibility#vuukle-comments-1980090

Fallière, N., O'Murchu, L., & Chien, E. (2011). W32.Stuxnet Dossier (Version 1.4). Mountain View: Symantec Security Response.

Frei, J. (2020). Israel's national cybersecurity and cyberdefense posture: Policy and organizations (Center for Security Studies Cyber-Defense Report). Zurich: Center for Security Studies, ETH Zurich.

Ghazizadeh, A. (2011). "The Impact of network society on intelligence organizations." Strategic Studies Quarterly, 14(3), 36–68.

International Institute for Strategic Studies (IISS). (2021). Cyber capabilities and national power: A net assessment, 6. Israel. London: IISS.

Kaminska, M., Cristiano, F., & Broeders, D. (2021). Limiting viral spread: Automated cyber operations and the principles of distinction and discrimination in the gray zone. In T. Jančárková, L. Lindström, G. Visky, & P. Zotz (Eds.), Proceedings of the 13th International Conference on Cyber Conflict: Going Viral (pp. 59–72). Tallinn: NATO CCDCOE Publications.

Kingsley, J. (2023). Offensive cyber operations: States' perceptions of their utility and risks. London, UK: Royal Institute of International Affairs.

Kramer, F. D. (2009). Cyber power and national security: Policy recommendations for a strategic framework. In F. Kramer, S. H. Star, & L. K. Wentz (Eds.), Cyber power and national security. Dulles: National Defense University Press and Potomac Books.

Kuehl, D. (2009). From cyberspace to cyber power: Defining the problem. In F. Kramer, S. Starr, & L. Wentz (Eds.), Cyber power and national security. Dulles: Potomac Books.

Kwasich, G., & Buny, W. (2014). Network espionage: Global information threat (Research Deputy, Imam Baqir University, Trans.). Tehran: Imam Baqir University Press.

Matania, E., & Yoffe, L. (2022). Some things the giant could learn from the small: Unlearned cyber lessons the US could take from Israel. The Cyber Defense Review, winter 2022, 101–109. Carlisle, PA: The Cyber Defense Review.

Mazarr, M. (2002). Information technology and world politics. New York: Palgrave Macmillan.

Microsoft. (2024). Iran accelerates cyber ops against Israel from chaotic start. Redmond, WA: Microsoft.

Nye, J. (2011). The future of power. Philadelphia, PA: Public Affairs.

Passive Defense Organization. (2015). "Mission, goals, and duties of cyber defense." PAPSA Monthly, 9, 1–36.

Reuters. (2021, October 26). Iran says cyberattack behind widespread disruption at gas stations. London: Reuters. Retrieved from https://www.reuters.com/world/middle-east/iran-says-cyberattack-behind-widespread-disruption-gas-stations-2021-10-26/

Rosenau, J. N., & Singh, J. P. (2002). Information technologies and global politics: The changing scope of power and governance. New York: State University of New York Press.

Sean, C. (2019). The Israeli Unit 8200 – An OSINT-based study. Center for Security Studies (CSS), ETH Zürich, CSS Cyber Defense Trend Analyses. https://doi.org/10.3929/ethz-b-000389135

Sheldon, J. (2012). Toward a theory of cyber power: Strategic purpose in peace and war. In Cyberspace and national security: Threats, opportunities, and power in a virtual world (pp. 207–224).

Siman, D., & Even, S. (2020). A new level in the cyber war between Israel and Iran (INSS Insight No. 1328). Institute for National Security Studies. Retrieved from https://www.jstor.org/stable/resrep25542

Torabi, G. (2016). "Assessment of the Israeli military strategy." Strategic Studies Quarterly, 19(3), 160–166.

Trellix. (2024). The Iranian cyber capability (Threat research report). Milpitas, CA: Trellix.

Utinková, H. (2021). Cyber-attacks against Iran as instruments of hybrid warfare (Master's thesis). Charles University, Faculty of Social Sciences, Institute of Political Studies, Department of Security Studies. Retrieved from https://dspace.cuni.cz/bitstream/handle/20.500.11956/127643/120387271.pdf?sequence=1&isAllowed=y

Wired, T., (2024, January 25). How a group of Israel-linked hackers has pushed the limits of cyber war. New York: Wired Media. Retrieved from https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/

Wister, F., (2004). Theories of the information society (E. Ghadimi, Trans., 2nd ed.). Tehran: Ghasedeh Sara Publishing.

Zafari, H., Najafi, R., & Zafari, H. (2021). Instruments of power in cyberspace. Tehran: Arshdan Educational Institute.

Zetter, K. (2015). Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. New York: Crown.