



Article Type: Research paper

Cyberspace in Israel's Offensive and Defence Military Strategy from the Perspective of Upstream Documents

* Seyed Amin Habibi¹, Arefeh Abbasi Karafshani²

1. Ph.D. in International Relations, visiting professor at Islamic Azad University, Science and Research Branch, Tehran, Iran
2. Graduated Political science and International relations Researcher, Islamic Azad University, Science and Research Branch, Tehran, Iran

Article Info.

Received: 4/10/2024

Accepted: 2024/11/25

Available Online: 10/3/2025

Abstract

The emergence of new security threats and the concept of comprehensive security have presented significant challenges to regional actors. Over the past decade, cyberspace has become one of the most critical battlegrounds. While offering immense opportunities for humanity, it has also introduced novel threats and serious challenges to human security. Israel, recognizing the importance of cyberspace, has invested heavily in both defensive and offensive strategies to address its geopolitical vulnerabilities. This study aims to explore the role of cyberspace in Israel's military strategies by analysing its strategic documents. The findings reveal that Israel has established close collaboration between military-security institutions and private cybersecurity companies, creating a unified framework to address both offensive and defensive dimensions. This approach has enabled Israel to control cyber threats effectively and

Seyed Amin Habibi, Ph.D.

Address: Ph.D. in International Relations, visiting professor at Islamic Azad University, Science and Research Branch, Tehran, Iran.

E-mail: se.aminhabibi@gmail.com

How to Site:

Habibi, Seyed Amin and Abbasi Karafshani, Arefeh. (2025). Cyberspace in Israel's offensive and defence military strategy from the perspective of upstream documents. *Fundamental and Applied Studies of the Islamic World*, 6(4), 21-24.



Authors retain the copyright and full publishing rights.
Published by Iranian Association of Geopolitics. This article is an open access article licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0)

establish cyber deterrence. With the expansion of globalization, the technological revolution, and the pervasive influence of the internet across all aspects of governance, economy, and culture, cybersecurity has emerged as a central focus of security studies. The rise of new threats and opportunities in this domain has compelled states to establish regulatory frameworks and policy measures to maintain stability and manage crises. In international relations, cybersecurity encompasses a set of policies, decision-making processes, and strategies aimed at identifying, monitoring, and mitigating cyber threats. In today's world, cybersecurity has become a necessity for states, and effective governance is impossible without considering this domain. Deterrence, a key security strategy, is applicable in military, missile, space, and cyber domains. This theory initially emerged during the Cold War to describe the impact of nuclear weapons in preventing direct conflict. Today, the concept of deterrence has expanded to include economic, informational, espionage, technological, and media tools, referred to as modern deterrence. The characteristics of cyber deterrence include its punitive nature, whereby a nation's cyber capabilities can instill fear in adversaries and deter hostile actions. Moreover, cyber deterrence extends beyond the cyber domain, as it can also prevent adversaries from engaging in physical, missile, and espionage attacks. Additionally, this strategy allows for responses to security-military threats to be carried out both traditionally (militarily) and through cyber means. Consequently, the cyber domain has not only become a new arena for security-military competition but has also provided new tools for establishing deterrence at the international level. Israel has strategically planned its cyber policies across four dimensions: economic, military-intelligence, social, and political. By leveraging its cyber capabilities, Israel has expanded its intelligence, espionage, and sabotage operations regionally and globally. The unique characteristics of cyberspace, such as its vast networked infrastructure and high-speed data transmission, have allowed Israel to enhance its military capabilities and shift the balance of power. Facing existential threats, Israel has prioritized cyberspace, making substantial investments in this domain. With 12% of the world's top 500 cybersecurity companies and 470 active start-ups, Israel is the second-largest cybersecurity hub globally. In 2021, its cybersecurity exports were three times higher than those of the UK. Cyberspace comprises three layers—human, software, and physical—each of which can be targeted for offensive or defensive purposes. Cyberattacks can manipulate user behaviour, infiltrate software for espionage, or disrupt physical infrastructure, such as power plants or aviation systems. This study examines Israel's strategic documents and its offensive and defensive cyber strategies. The

hypothesis is that Israel has implemented comprehensive strategies by coordinating military-security institutions and private companies, effectively controlling cyber threats. Israel's cyber strategies are analysed across four dimensions, and its capabilities have enabled it to expand its intelligence, espionage, and sabotage operations globally. The research methodology is based on document analysis and descriptive research, with findings presented in five sections: the role of cyberspace in Israel's strategic documents, defensive and offensive approaches, workforce development, and cyberspace's role in Israel's broader military strategies. Given the diverse security threats it faces, the strategic importance of cyberspace, and its heavy reliance on the presence and management of this domain, Israel has adopted two overarching approaches in its cybersecurity documents: cyber defence and cyber offense. In analysing Israel's strategic documents, cyberspace is characterized by several components, including a domain for foreign infiltration and attacks, a tool for effective governance and management, a driver of economic development and growth, and a factor contributing to social welfare and stability. However, the most prominent and significant component among these diverse aspects is the emphasis on defence and military affairs. Numerous governmental and private institutions in Israel operate in the defensive sphere of cyberspace. The entities responsible for cybersecurity in the regime aim to monitor and control institutions that provide essential services in the occupied territories and are responsible for the administrative procedures and daily lives of the residents. Consequently, attacks on these institutions impact public morale, order, governance methods, and the regime's legitimacy. From Israel's perspective, as briefly outlined in its strategic and high-level documents, the sources of cyber threats are multifaceted and include non-aligned countries, hostile governments, terrorist organizations, hackers, and even private individuals. The importance of cyberspace is undeniable, as states use it to enhance governance. For Israel, cyberspace is vital both militarily and non-militarily. Due to its lack of strategic depth and ongoing regional conflicts, Israel faces geopolitical constraints, necessitating diverse military measures. Cyberspace offers Israel a strategic advantage, and over the past two decades, it has focused on developing human capital, legislation, and institutional frameworks to strengthen its cyber capabilities. Collaboration with Western partners, particularly the United States, has positioned Israel as a influential cyber actor in the region. Israel has enhanced its cyber capabilities in both offense and defence, utilizing cyberspace in military-intelligence strategies during regional conflicts, such as Operation Orchard and the 2014 Gaza conflict. The study highlights the significance of cyberspace in Israel's military

strategies, evident in its numerous cyber-related institutions, including the Cyber Directorate. A clear division of responsibilities exists among Israel's branches of government for cyber defence. Israel's cyber capabilities and technological advancements aim to establish cyber deterrence against regional threats. Successful cyberattacks and espionage operations have contributed to this deterrence. The diversification of threats and the concept of comprehensive security have led Israel to expand its military operations, opening new fronts against adversaries. Israel's legislative and strategic frameworks for cyberspace are noteworthy. The first legislative action in this domain was the 1998 "Security Regulations in Government Institutions," which defined responsibilities for information and computer security in public institutions. In 2015, Israel established the National Cyber Directorate under the Prime Minister's Office to oversee cyber policies and implement recommendations. The Directorate is responsible for research and development, emergency tools, and cybersecurity frameworks. In 2015, the Israeli Defence Forces (IDF) assigned cyber operations to two units: Unit 8200 for offensive operations and the Computer Service Directorate for defence. Other institutions, such as the Finance Ministry's Computer Division, the Police Cyber Unit, and the Ministry of Justice, also play roles in cybersecurity. Israel's strategic investments in cyberspace have positioned it as a global cyber power. Its high export capacity in cybersecurity products generates significant economic benefits for private companies while enhancing its espionage and sabotage capabilities. Militarily, Unit 8200, staffed by elite university graduates, has conducted numerous cyber operations against various countries, including Iran. However, groups like Hezbollah have countered Israel's cyber deterrence, exposing its vulnerabilities. Israel's reliance on cyberspace extends to its economy, and its aggressive cyber strategies aim to compensate for its lack of political legitimacy and strategic depth. By targeting various countries, Israel seeks to achieve multiple objectives through cyberspace. In conclusion, Israel's strategic focus on cyberspace has enabled it to address its geopolitical challenges, establish cyber deterrence, and expand its influence globally. Its comprehensive approach, combining military, economic, and technological strategies, underscores the critical role of cyberspace in its national security framework.

Key words: Cyber space, Israel, military strategies, national security, wide Security.