MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Commentary

The 12-Day War: Cyber Frontlines between Israel and Iran

Rohit Kumar Sharma

August 11, 2025

Summary

The Islamic Republic struggled to protect its critical infrastructure, whereas Israel emerged largely unscathed in the cyber domain during the 12-Day War.

Cyber offensive operations have become an integral part of contemporary military conflicts. States also increasingly rely on these operations to project power, shape narratives and undermine the adversaries' infrastructure. States' tendency to leverage the cyber realm for tactical and strategic objectives further underscores its significance in modern conflicts. The synchronisation of cyber campaigns with kinetic operations also indicates cyberwarfare's evolving nature, which is not merely perceived as a set of 'grey-zone' tactics operating between peace and war but as an integral part of armed conflict.

The trend of conducting cyber offensive operations simultaneously with military hostilities was very evident in the '12-day war' between Israel and Iran. Following Israel's 'pre-emptive' strikes against Iran's nuclear and ballistic missile programme, an Iranian retaliation through cyberattacks was widely anticipated.[1] Cyber operations were a more viable alternative for Iran, given the vast schism between Israeli and Iranian military capabilities, with Tel-Aviv leading in advanced conventional military strength. For Israel, cyber operations essentially served its intelligence gathering and reconnaissance missions over the Iranian nuclear and ballistic programme.[2]

Israel–Iran Escalation in 'Bits and Bytes'

Before initiating conventional strikes, Israel relied on cyber operations to turn off Iranian radar systems and military communications, enabling successful strikes by the Israeli Air Force (IAF) without any resistance.[3] Shortly after the Israeli military campaign was made public, there was a surge in activities on Telegram channels, including coordinated propaganda and mobilisation efforts by threat actors that were believed to be aligned with Iran.[4] Several of these groups issued warnings against Israel's neighbours, threatening consequences if they supported Israel, while others made unverified claims of successful cyber operations against Israeli infrastructure.[5]

During the initial days of the conflict, threat actors sympathetic to or believed to be aligned with Israel and Iran were observed escalating their activities. The most

[1] **"Heightened Cyberthreat Amidst Israel-Iran Conflict"**, *Radware*, 13 June 2025.

[2] Susan Greene, **"Inside Israel's Unit 8200: The Team of Teen Tech Whizzes Who Tracked Down Iran's Uranium Enrichment Sites"**, *Daily Mail,* 23 June 2025.

[3] Bilal Y Saab and Darren D. White, **"Lessons Observed from the War Between Israel and Iran"**, *War on the Rocks*, 16 July 2025.

[4] **"Heightened Cyberthreat Amidst Israel-Iran Conflict"**, no. 1.

[5] Ibid.

notable Israel-linked group, *Gonjeshke Darande* (Persian for Predatory Sparrow), which has a history of targeting Iran, publicly claimed its involvement in a cyber incident against Iranian financial institutions.[6] The group also claims that it targeted the 'oppressive regime' in Iran, while emphasising minimal civilian harm.[7]

Pro-Israel groups carried out high-impact cyber operations targeting Iran's financial infrastructure, including a major cryptocurrency heist valued at US$ 90 million. The attack on Iran's banking services appears to be a calculated effort to undermine the country's financial stability, which has already been under strain due to international sanctions.

Over the years, multiple assessments have suggested a sophisticated network of Advanced Persistent Threats (APTs) linked to Iran.[8] The Iranian government has used these APTs to engage in espionage and disruptive activities.[9] During the 12-day conflict, pro-Iranian groups surged in cyber activity, outnumbering their pro-Israeli counterparts. However, despite their volume, these groups fell short in terms of impact and were largely unsuccessful in causing significant damage to Israeli systems.

Many of the claims made by pro-Iranian hackers were either denied by Israeli authorities or appeared to be overstated in terms of scope (see Table 1). In one case, Pay2Key.I2P, an Iranian-backed ransomware-as-a-service (Raas) group, offered up to 80 per cent profit shares of ransom payments to affiliates willing to conduct cyberattacks against Israel and the US.[10] OSINT sources indicate the emergence of new threat actors such as Blacksword, Night Hunters, Tunisian Maskers Cyber Force, and others that were seen actively amplifying the agendas of the states involved in the conflict, further blurring the distinction between state-sponsored operations and decentralised digital warfare.[11] Iranian hackers also made several attempts to breach internet-connected security cameras in Israel to gather real-time

[6] **"Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel-Iran War"**, *Radware*, 18 June 2025.

[7] Jeremy Makowski, "Israel-Iran War: Cyber and Electronic Warfare Operations", June 2025.

[8] Ibid.; **"IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities"**, Cybersecurity and Infrastructure Security Agency (CISA), 18 December 2024.

[9] **"Home Iranian APTs: An Overview Iranian APTs: An Overview"**, Middle East Institute, 10 February 2023.

[10] Ilia Kulmin, **"Pay2Key's Resurgence: Iranian Cyber Warfare Targets the West"**, *Morphisec*, 8 July 2025.

[11] Jeremy Makowski, "Israel-Iran War: Cyber and Electronic Warfare Operations", no. 7.

intelligence to adjust missile targeting. This tactic also closely resembles methods used during the Russia–Ukraine war.[12]

Table 1. Israel–Iran escalation in Cyberspace*

Threat Actor	Target/Victim	Attack Type/Method
Israel		
Unknown actors (potentially linked to Israel/Pro-Israel/ anti-Iranian regime hackers, not related to Israel)	Iran's digital infrastructure from the morning of Friday, 13 June	The exact nature is unknown, but Iran's cyber command ordered top officials and security teams to avoid IT equipment.[13]
Predatory Sparrow	Sepah bank (Iran)	Data wiping attack; network disruption[14]
Unknown actors (potentially linked to Israel/Pro-Israel/anti-Iranian regime hackers, not related to Israel)	Pasargad bank (Iran)	DDoS attack[15]
Predatory Sparrow	Nobitex cryptocurrency exchange (Iran)	Data wiping attack, theft, and destruction of cryptocurrency[16]
Tapandegan	Bank Mellat (Iran)	Data leak[17]
Unknown actors (potentially linked to Israel/Pro-Israel/ anti-Iranian regime hackers, not related to Israel)	The Islamic Republic of Iran Broadcasting (IRIB) was hacked. Attackers took control of the live transmission and replaced content with anti-regime footage.	System intrusion, also part of a larger psychological operation against the Islamic Republic

[12] Daryna Antoniuk, **"Israeli Officials Say Iran Exploiting Security Cameras to Guide Missile Strikes"**, *The Record*, 23 June 2025.

[13] Antoaneta Roussi and Dana Nickel, **"Iran Orders Officials to Ditch Connected Devices"**, *Politico,* 17 June 2025.

[14] Michael Doran and Zineb Riboua, **"Predatory Sparrow Hacks Iran's Financial System"**, *The Wall Street Journal,* 20 July 2025.

[15] **"Banking Disruptions Persist in Iran After Cyberattacks Target Major Banks"**, *Iran International*, 29 June 2025.

[16] Ibid.

[17] **"Hackers Hit Iran's Bank Mellat, Leak Data on Millions"**, *Iran International*, 24 June 2025.

Iran		
Hacktivists collective APT Iran	Targeted servers associated with the Israeli government and private entities	Prominent ransomware strains from ALPHV and Lockbit were used to cause widespread disruption. No significant disruption is linked to this report.[18]
"Handala group" with alleged Iranian state backing[19]	Hackers claimed to have stolen over two terabytes of data from Israel's petroleum conglomerate, the Delek group, and its Delkol subsidiary. The group also listed other Israeli entities from the construction sector, an internet service provider, and an Argentinian drone manufacturer accused of working with the IAF.[20]	Data breach and leak. The extent of the breach is believed to be overstated.[21]
Threat actors like Mr. Hamza, Team Fearless, and Arabian Ghosts	Multiple public sector, government, and defence institutions	DDoS attacks and website intrusions[22]
Iranian state-sponsored APT34 (OilRig) and APT39 (Remix Kitten)	Israeli government and defence networks	Cyber espionage, phishing, and zero-day exploits[23]
Pro-Iranian group #OpIsrael	Tzofar—Israel's public alert system	The group claimed the attack without any substantiating evidence.[24]

[18] **"Flash Report: Israel-Iran Cyber Threat Landscape"**, *Zerofox*, 26 June 2025.

[19] **"Handala Hacking Group Asserts Attacks Against Israel"**, *SC Media*, 17 June 2025.

[20] Ibid.

[21] David Hollingworth, **"Pro-Palestinian Hackers Target Israel in Wake of Attack on Iran"**, *cyberdaily.au*, 16 June 2025.

[22] **"The Hacktivist Cyber Attacks in the Iran-Israel Conflict"**, NSFOCUS, 26 June 2025.

[23] **"Heightened Cyberthreat Amidst Israel-Iran Conflict"**, no. 1.

[24] Ibid.

IRGC-linked Educated Manticore	Targeted Israeli journalists, high-profile cybersecurity professionals, and professors	Spear-Phishing[25]
Unknown pro-Iran hackers	Security cameras in Israel	Intrusion due to weak passwords, outdated firmware, and poorly configured systems[26]

*The table includes only public cyber incidents that are not chronologically arranged.

Source: Prepared by the author from Media Reports.

A flood of influence operations across social media platforms, ubiquitous in contemporary conflicts, also marked the conflict. These influence operations were overwhelmingly infused with AI-generated content, significantly compounding the scale and impact of the information warfare.[27] Accounts linked to Iran or pro-Iranian actors were seen attempting to spread panic in Israel by posting messages in Hebrew, while accounts tied to Israel circulated content in Persian, aimed at undermining the Iranian government's authority among its citizens.

Following the US attack on Iranian nuclear facilities, American authorities also anticipated an Iranian cyber offensive against its critical infrastructure. Concerns regarding possible Iranian cyber offensive operations were widely shared by various US agencies, including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA).[28] The fact sheet also placed the Defence Industrial Base companies at high risk in association with Israeli research and defence firms.[29]

Looking at the nature of operations and the type of targets, the intent appears to have been to disrupt civilian life and erode public confidence in their respective governments. The sophisticated attacks conducted by groups like Predatory Sparrow

[25] **"Iranian Educated Manticore Targets Leading Tech Academics"**, *CheckPoint*, 25 June 2025.

[26] Daryna Antoniuk, **"Israeli Officials Say Iran Exploiting Security Cameras to Guide Missile Strikes"**, no. 12.

[27] Steven Lee Myers, Natan Odenheimer and Erika Solomon, **"Israel and Iran Usher In New Era of Psychological Warfare"**, *The New York Times*, 15 July 2025.

[28] **"Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest"**, CISA, 30 June 2025.

[29] Ibid.

indicate the likely involvement of state actors while allowing groups to maintain plausible deniability.

Another noteworthy development was the Iranian government's use of complete internet blackouts as a defence mechanism, illustrating the absence of adequate domestic cybersecurity preparedness. The inadequacy also emanates from international sanctions over Iran's digital ecosystem, which has increased the risk of data breaches and cyberattacks against its systems.[30] The vulnerabilities increase as Iranians rely on insecure Virtual Private Networks to circumvent government filters, leaving them defenceless against threat actors.[31]

One peculiar aspect of cyberspace is that threat actors often continue to engage even after conventional hostilities have ceased. While there was a noticeable decline in cyber activity following the ceasefire, offensive operations in the cyber realm did not completely halt. While direct military confrontation between Israel and Iran was unprecedented, cyber offensive operations did not represent a significant shift in the way cyber warfare has traditionally been conducted between the two states. These operations provided an "incremental edge" in the conflict, rather than producing an outcome with profound strategic utility.[32] Although there was no clear winner in the Israel–Iran cyber conflict, the Islamic Republic struggled to protect its critical infrastructure, whereas Israel emerged largely unscathed. Both nations will likely continue employing cyber operations as part of gray zone tactics until the subsequent escalation.

[30] Imad Payande, **"Breaking the Web: How Sanctions Are Undermining Iran's Access to the Internet"**, *Internet Society*, 26 November 2024.

[31] Ameneh Dehshiri, **"The VPN Epidemic in Iran: A Digital Plague Amid Global Isolation"**, *Stimson*, 9 September 2024.

[32] Nikita Shah, **"What the Israel-Iran Conflict Revealed About Wartime Cyber Operations"**, Atlantic Council, 30 July 2024.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses