Author

Megi Benia

The Cyber Dimension of the Israel-Iran War: Implications for Regional Security and Modern Warfare

23/09/2025

The Cyber Dimension of the Israel-Iran War: Implications for Regional Security and Modern Warfare

Author: Megi Benia, UGSPN Affiliated Fellow

Abstract

The June 2025 Israel-Iran War introduced a new and alarming dimension to regional conflict: the deep integration of cyber warfare with conventional kinetic strikes. This paper examines the cyber operations launched by both states during the brief but intense conflict, detailing their targets, methods, and strategic effects. It analyzes how Israel targeted Iranian financial and maritime infrastructure while Iran responded with disruptive attacks, disinformation, and widespread surveillance manipulation. The study then explores the profound implications of this digital battlefield for regional security, modern military doctrine, international law, and escalation dynamics. Based on open-source intelligence and expert analysis of pre-existing capabilities, the paper traces how both nations leveraged their cyber arsenals not just as tactical tools but as potent psychological weapons. The digital spillover into neighboring Gulf states and the deliberate, although limited, nature of the attacks highlight the emergence of new, unwritten rules of engagement. The paper concludes with lessons learned, which can pave the way to develop robust deterrence strategies, resilience frameworks, and diplomatic norms adequate to meet the challenges of future hybrid wars, where the digital front is inseparable from the physical one.

Introduction

The conflict that erupted between Israel and the Islamic Republic of Iran in June 2025 was, by conventional metrics, a short war. Lasting twelve days, it was characterized by a rapid and devastating series of Israeli air strikes under the code name “Operation Rising Lion”, followed by a retaliatory barrage of Iranian ballistic missiles aimed at strategic targets in Israel. The fighting was triggered by a significant escalation in proxy violence in Syria and Lebanon, culminating in a direct state-on-state confrontation that the world had long feared. While the kinetic exchanges were intense and captured global headlines, a parallel and equally significant war was being waged in the digital domain. This was not a sideshow but a core component of the strategy for each nation, marking a breakpoint moment in the history of modern warfare in the Middle East.

For years, Israel and Iran had engaged in a "shadow war" in cyberspace, a persistent, low-level conflict of sabotage, espionage, and disruption (Warrick 2021). However, the June 2025 war saw these operations move from the shadows into the harsh light of an active battlefield. Cyberattacks were no longer just tools of attrition or signaling, they became force multipliers, directly integrated with military operations to achieve strategic, operational, and psychological objectives. Israel used cyber capabilities to degrade Iran's ability to finance its war effort and command its forces, while Iran deployed its digital arsenal to sow chaos, spread fear, and demonstrate its reach far beyond its borders.

This paper examines the cyber dimension of the June 2025 war to uncover its broader implications for regional security and the future of modern warfare. It begins by analyzing the offensive cyber operations launched by both Israel and Iran, followed by an exploration of the key actors behind these

actions, including state-sponsored advanced persistent threat (APT) groups and affiliated hacktivist networks. The analysis then turns to the immediate and long-term consequences of the conflict, highlighting issues such as digital spillover and the destabilizing effects of cyberattacks beyond the battlefield. In doing so, the paper illustrates how this confrontation reshaped strategic thinking around escalation, deterrence, and the role of cyberspace in warfare. Building on these findings, it offers policy recommendations aimed at helping governments and international organizations adapt to the realities of an increasingly contested and integrated cyber domain. Finally, the conflict cemented cyberspace as a decisive arena of modern conflict that demands new frameworks for defense, diplomacy, and international stability.

Cyber Operations During the War

The digital operations in the June 2025 war were notable for their synchronicity with kinetic military action. Rather than being opportunistic or coincidental, the attacks appear to have been designed to complement physical strikes at decisive moments. On the one hand, Israel's cyber operations appeared to be highly coordinated with its air campaign, "Operation Rising Lion". The primary objective was to cripple Iran's economic and logistical backbone. One of the most significant strikes targeted Iran's financial infrastructure, with a particular focus on institutions linked to the Islamic Revolutionary Guard Corps (IRGC). Bank Sepah, a state-owned bank with deep ties to the IRGC and already under international sanctions, experienced a notable systems failure on June 16, 2025, halting transactions and erasing customer data (The Times, June 17, 2025). Simultaneously, Nobitex, Iran's largest cryptocurrency exchange, was hit by a sophisticated attack that locked users out of their wallets and sowed panic among a population increasingly reliant on digital assets to evade sanctions (AP News 2025; Guardian 2025; TRM Labs 2025; Greenberg 2025). Beyond finance, Israeli electronic warfare units executed a widespread GPS jamming and spoofing campaign in the Strait of Hormuz (IntelliNews 2025). This action created chaos for commercial shipping, misdirecting vessels and causing near-collisions, demonstrating an ability to disrupt global trade at a critical chokepoint without firing a shot (Reed 2025).

Iran's response, while less technologically precise, was broad and aimed at creating psychological terror and demonstrating resilience. Iranian cyber units launched massive Distributed Denial-of-Service (DDoS) attacks against Israeli government websites, news outlets, and emergency service portals, creating confusion and disrupting public access to information. In a move designed for maximum public impact, Iranian hackers hijacked thousands of public and private CCTV cameras across Israel, replacing live feeds with propaganda videos and displaying messages of intimidation on digital billboards in Tel Aviv and Haifa (Ben Am and Fixler 2025). This tactic, while causing no physical harm, created a powerful sense of vulnerability among the Israeli public. Iranian actors also targeted industrial systems, causing minor disruptions at a water desalination plant in southern Israel before automated safety systems restored control, hinting at a more destructive capability held in reserve (Ben Am and Fixler 2025).

Targets, Actors, and Capabilities

The cyberattacks during the June 2025 war were carried out by a complex network of state-sponsored groups, cover units, and an army of non-state proxies. Understanding these actors is key to deciphering the conflict's digital structure.

Israel's offensive operations were widely attributed to its elite intelligence units, particularly Unit 8200 of the Israeli Defense Forces (IDF), renowned for its offensive cyber capabilities (Olech and Kwaśniewska 2025). Publicly, however, responsibility was often claimed by a hacktivist front group known as "Predatory Sparrow" (Greenberg 2025). This group had a prior history, having claimed responsibility for a 2022 cyberattack that caused a fire at an Iranian steel mill (Times of Israel 2022). In the 2025 war, Predatory Sparrow served as a tool for plausible deniability, allowing Israel to acknowledge its actions ambiguously while avoiding direct state-on-state confirmation (Greenberg 2025; Vicens 2025). The precision of the group, its focus on industrial control systems (ICS), and its alignment with Israeli strategic interests left little doubt among intelligence analysts about its state affiliation (Radware 2025).

On the Iranian side, the cyber effort was spearheaded by the IRGC's Cyber Command, which oversees a constellation of APT groups. These groups, often tracked by Western cybersecurity firms under names like APT33 (Elfin), APT34 (OilRig), and APT39 (Chafer), have a long history of espionage and disruptive attacks targeting rivals in the Middle East and beyond (Mandiant 2022). During the war, these state-sponsored entities focused on high-value targets, such as the attempted breach of the Israeli desalination plant (Radware 2025; VeriTech Consulting 2025). However, a significant portion of Iran's strategy relied on a vast network of hacktivist proxies.

The conflict triggered a surge in hacktivist activity, with over 120 distinct groups joining the fray. Pro-Iranian groups like "Noname057(16)", a nominally pro-Russian group that expanded its operations, Mr. Hamza Group, Keynous+, and the Mysterious Team Bangladesh launched low-sophistication but high-volume attacks against Israeli and allied websites (Radware 2025; VeriTech Consulting 2025). Their purpose was to create a "fog of war" in cyberspace, flooding security operation centers with alerts and distracting them from the more serious state-sponsored intrusions. These groups also expanded the conflict's geography, targeting government and commercial entities in the United States and several European nations perceived as supporting Israel, thereby internationalizing the digital front. This decentralized, proxy-based model provides Iran with both operational scale and a layer of deniability, complicating attribution and response.

Regional Security Implications

The cyber dimension of the June 2025 war had profound and destabilizing implications for the entire Middle East, demonstrating that digital attacks, like radiation, do not respect national borders. The conflict created a significant "digital spillover," threatening the stability and neutrality of neighboring states.

One of the most immediate effects was felt in the Gulf. As Israel and Iran battled for digital supremacy, internet traffic and data services in nearby countries were caught in the crossfire. In Qatar and the UAE, thousands of mobile phone users reported their geolocation services being misrouted, a side effect

of the intense electronic warfare and GPS spoofing centered on the Strait of Hormuz (Arab Times Online 2025). Critical infrastructure in Gulf states, which often relies on the same software, hardware, and undersea cables as the belligerents, faced an elevated risk of collateral damage. A minor disruption at a Saudi Arabian petrochemical facility, for instance, was later traced back to malware that had propagated from the Iranian network during the conflict, underscoring the interconnectedness and vulnerability of the region's infrastructure (Windward 2025).

The attacks on maritime security in the Strait of Hormuz represented a direct threat to the global economy and regional stability. By demonstrating an ability to disrupt one of the world's most vital energy arteries through non-kinetic means, the conflict set a dangerous precedent. Future regional crises could see similar tactics employed, holding global energy markets hostage and threatening freedom of navigation. This forces regional states and international maritime coalitions to invest heavily in electronic hardening and alternative navigation systems, adding a new layer of complexity to maritime security operations.

More broadly, the war undermined the concept of third-party neutrality. The proliferation of hacktivist proxies, launching attacks from and against countries not directly involved in the war, eroded the line between combatants and non-combatants in the digital realm. This created a heightened risk of a chain-reaction cyber conflict, where an attack on a neutral Gulf state could be misattributed, leading to retaliatory strikes and escalating a bilateral conflict into a regional conflagration. The June 2025 war thus left the Middle East a more volatile and unpredictable place, where digital vulnerabilities could easily become catalysts for wider physical conflict.

Modern Warfare and Escalation Dynamics

The June 2025 war provided a clear and compelling case study of cyber power as a force multiplier in a short-duration, high-intensity conflict. It also offered crucial, if unsettling, insights into escalation management in the digital age.

The synergy between cyber operations and the kinetic air campaign was a defining feature of Israel's strategy. By disrupting Iranian financial networks before and during „Operation Rising Lion", Israel aimed to hamper Iran's ability to mobilize and sustain its military response. The GPS jamming in the Strait of Hormuz served to distract and divert Iranian naval attention, creating a more permissive environment for Israeli forces operating elsewhere. These cyber effects were achieved at a fraction of the cost and political risk of equivalent kinetic strikes, such as bombing a bank or blocking a port. This demonstrated a mature military doctrine where cyber is no longer a preparatory tool for conflict, but a co-equal instrument of power wielded alongside air, sea, and land forces.

Despite the intensity of the attacks, both sides appeared to exercise a degree of restraint. However, whether this reflects tacit norms or technical constraints remains open to debate. Iran's cyber operation against a desalination plant, for example, was halted before it caused lasting damage or endangered civilian water supplies, but it is unclear if this was due to policy decisions, operational capability, or technical limitations. Similarly, no confirmed cyberattacks targeted hospital life-support systems or air traffic control to produce mass casualties, echoing restraint observed in earlier state-on-state cyber confrontations such as Stuxnet or the 2017 NotPetya incident, where certain critical civilian

infrastructures were also avoided. While such patterns hint at an emerging understanding that weaponizing some types of critical infrastructure risks dangerous escalation, they could also indicate caution in untested dimensions. This restraint remains fragile, contingent on both technical capacity and rational decision-making, leaving open the possibility of future miscalculation.

The conflict also highlighted the persistent challenges of attribution, deterrence, and ambiguous thresholds. While intelligence agencies could attribute the major attacks to state actors, the use of proxies like Predatory Sparrow and the swarm of hacktivists created a public narrative of ambiguity. This complicates deterrence: how can a state deter an action if the perpetrator can plausibly deny it? The United States, concerned about spillover attacks on its own infrastructure, issued public warnings to both sides and reportedly used intelligence channels to clarify attribution for key attacks, signaling that a digital "fog of war" would not prevent a response if American interests were threatened. This underscored the need for robust, shareable attribution mechanisms to maintain deterrence stability in a world of hybrid warfare.

Lessons Learned

June 2025 The Israel-Iran war revealed several key lessons about the role of cyber operations in modern warfare and regional security. These lessons, drawn from the experience of both parties and the wider regional impact, provide important insights for governments, militaries, and international organizations.

- **Cyber power must be integrated into overall strategy.** The war demonstrated that cyber operations are most effective when synchronized with kinetic actions. Israel's coordinated strikes on Iranian financial infrastructure alongside air campaigns showed how cyber effects can amplify military objectives. Future military engagements will demand commanders trained to employ cyber capabilities as a routine instrument of power rather than as an ancillary tool.
- **Attribution remains a central challenge for deterrence**. The heavy use of proxies and hacktivist groups blurred responsibility and complicated decision-making. This ambiguity undermined traditional deterrence mechanisms and highlighted the urgent need for better, faster attribution methods.
- **Critical infrastructure is an attractive but vulnerable target.** Financial systems, maritime navigation, energy production, and water facilities emerged as priority targets during the war. Both states exercised restraint, but the ease with which these systems were disrupted underscores the importance of resilience, robust deterrence, and air defense systems to protect civilian life and economic stability.
- **Escalation management depends on tacit "red lines."** Despite the high stakes, both Israel and Iran appeared to avoid cyberattacks likely to cause mass civilian casualties or long-term damage to essential services. This suggests emerging but fragile norms around targeting certain types of infrastructure, norms that need to be better articulated and institutionalized to avoid miscalculation.
- **Communication channels reduce miscalculations.** The conflict showed how quickly cyber operations can spiral across borders. The absence of formal "cyber hotlines" or crisis channels

increased the risk of misunderstanding and escalation.Establishing communication mechanisms is critical in preventing a minor incident from snowballing into a regional conflagration.

- **Regional and international cooperation is essential.** The war highlighted the spillover risks for neighboring states, particularly in the Gulf. Shared attribution centers, joint exercises, and region-wide cyber norms could help stabilize an increasingly contested digital domain.
- **Societal resilience and counter-disinformation efforts are crucial.** The hijacking of CCTV feeds and disinformation campaigns illustrated the psychological dimension of cyber warfare. Strengthening public digital literacy, independent fact-checking, and civil-society engagement proved essential to blunt the impact of manipulative content.

Conclusion

The Israel-Iran war of June 2025 was short-lived but transformative. It revealed, with unprecedented clarity, that cyber warfare is no longer an adjunct to conventional operations but a fully integrated and decisive domain of conflict. The cyber dimension of this war has reshaped our understanding of escalation, deterrence, and the vulnerability of interconnected societies.

The lessons drawn from this conflict are sobering but invaluable. The synergy between cyber and kinetic operations underscored the importance of integrating digital tools into national defense planning. The fragility of critical infrastructure, the difficulty of attribution, and the emergence of tacit "red lines" all highlight the need for more resilient systems, clearer norms, and effective communication channels. Just as importantly, the hijacking of public-facing technologies showed that the psychological impact of cyber operations can be as destabilizing as physical strikes, calling for stronger societal resilience and information integrity.

Taken together, these lessons provide a roadmap for adapting defense, diplomacy, and deterrence to a new era of hybrid conflict. If internalized, they offer the possibility of preventing future crises from escalating into uncontrolled cyber-kinetic wars. If ignored, they risk leading to a future where small-scale digital attacks cascade into regional or even global confrontations. The challenge now is to institutionalize these lessons, turning insights from a brief but consequential war into durable frameworks for security and stability in the cyber age.

References

AP News. “Hackers Say They Wiped Out $90 Million from Iran Cryptocurrency Exchange.” Associated Press, June 18, 2025. https://apnews.com/article/8febb3c9c2acf4de2894a7a8a92aa88c

Arab Times Online. 2025. “Rising Tensions: Bahrain and Qatar Hit by GPS Spoofing.” June 23, 2025. https://www.arabtimesonline.com/news/rising-tensions-bahrain-and-qatar-hit-by-gps-spoofing

Ari Ben Am and Annie Fixler. 2025. *Iran Launches Counterattacks in Cyberspace.* Policy Brief, Foundation for Defense of Democracies, June 17, 2025. https://www.fdd.org/analysis/2025/06/17/iran-launches-counterattacks-in-cyberspace

Bloomberg. 2025. “Iran Shuts Down Internet in Bid to Tackle Mounting Cyber Attacks,” June 19, 2025. https://www.bloomberg.com/news/articles/2025-06-19/iran-flicks-its-internet-kill-switch-as-cyber-attacks-mount

Greenberg, Andy. “Israel-Tied Predatory Sparrow Hackers Are Waging Cyberwar on Iran’s Financial System.” *Wired,* June 19, 2025. https://www.wired.com/story/israels-predatory-sparrow-hackers-are-waging-cyberwar-on-irans-financial-system

IntelliNews. “1,000 Ships GPS Jammed in Straits of Hormuz, Sending up Costs and Disrupting Deliveries.” *IntelliNews,* June 24, 2025. https://www.intellinews.com/1-000-ships-gps-jammed-in-straits-of-hormuz-sending-up-costs-and-disrupting-deliveries-387363

Internet Society Pulse. 2025. “Shutdown – Iran (Islamic Republic of).” *Internet Society Pulse* dashboard, accessed July 2025. https://pulse.internetsociety.org/en/shutdowns/limited-internet-in-iran

Mandiant. *APT42: A Prolific Iranian Espionage Actor Targeting Dissidents and Foreign Policy Interests.* Milpitas, CA: Mandiant, 2022. https://cloud.google.com/blog/topics/threat-intelligence/apt42-charms-cons-compromises

NetBlocks. " Internet disrupted in Iran amid fuel protests in multiple cities." *NetBlocks.org,* November 15, 2019. https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b

Olech, Aleksander, and Dorota Kwaśniewska. 2025. *Cyber Forces: Israel.* Defence24, Geopolitics section, accessed July 2025. https://defence24.com/geopolitics/cyber-forces-israel

Radware. 2025. *Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel–Iran War.* Threat Advisory, June 18, 2025. https://www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/

Radware/IndustrialCyber. 2025. “Hybrid Warfare as Cyberattacks and Disinformation Escalate in 2025 Israel Iran Conflict.” *IndustrialCyber Threat Report,* June 21, 2025. https://industrialcyber.co/threats-attacks/radware-reports-hybrid-warfare-as-cyberattacks-disinformation-escalate-in-2025-israel-iran-conflict/

Reed, Tristan. “How Israel-Aligned Hackers Hobbled Iran’s Financial System.” *The Wall Street Journal,* June 21, 2025. https://www.wsj.com/world/middle-east/how-israel-aligned-hackers-hobbled-irans-financial-system-fb1b0376

The Guardian. “Israel-Linked Group Hacks Iranian Cryptocurrency Exchange in $90m Heist.” *The Guardian,* June 18, 2025. https://www.theguardian.com/technology/2025/jun/18/israel-linked-group-hacks-iranian-cryptocurrency-exchange-in-90m-heist

Times of Israel. “Mess with Israel, You’ll Pay a Price, PM Warns after Iran Steel Plant Cyberattack.” *The Times of Israel,* June 29, 2022. https://www.timesofisrael.com/mess-with-israel-youll-pay-a-price-pm-warns-after-iran-steel-plant-cyberattack

The Times. 2025. “Iranian Bank Linked to Revolutionary Guard Hit by ‘Cyber Attack.’” June 17, 2025. www.thetimes.com/world/middle-east/israel-iran/article/cyber-attack-irgc-bank-sapah-q9jwdtnbz

TRM Labs. “Inside the Nobitex Breach: What the Leaked Source Code Reveals about Iran’s Crypto Infrastructure.” *TRM Labs,* June 22, 2025. https://www.trmlabs.com/resources/blog/inside-the-nobitex-breach-what-the-leaked-source-code-reveals-about-irans-crypto-infrastructure

VeriTech Consulting. 2025. *June 2025 Cyber Conflict Update: Israel–Iran Tensions Escalate in Cyberspace.* Cyber Threat Intelligence Summary. https://www.veritech.consulting/cyber-activities-in-the-israel-iran-conflict-june-2025/

Vicens, A. J. 2025. “Iran crypto exchange hit by hackers, $90 million destroyed.” *Reuters,* June 18, 2025. https://www.reuters.com/world/middle-east/iran-crypto-exchange-hit-by-hackers-90-million-destroyed-2025-06-18/

Warrick, Joby. "Iran and Israel wage a shadow war of sabotage and cyberattacks." *The Washington Post,* April 13, 2021.

Windward. 2025. *Middle East on the Precipice: GPS Jamming in the Arabian Gulf and Strait of Hormuz Disrupts 970 Ships Daily.* June 19, 2025. https://windward.ai/blog/middle-east-on-the-precipice-gps-jamming-in-the-arabian-gulf-and-strait-of-hormuz-disrupts-970-ships-daily