Signal, Sabotage, Silence: Cyber Operations in the Israel–Iran War

September 1, 2025

In the shadow of bombs and missiles, Israel and Iran also waged a quieter battle online. From defacements and DDoS storms to deep-cover spyware and wholesale internet blackouts, each side tested its digital arsenal—yet none unleashed a knockout cyber strike. Instead, what emerged was a mosaic of incremental tactics, each aimed at shaping perceptions, sowing disruption, and gathering intelligence without decisively tilting the military balance.

The conflict's five core cyber segments:

- **The hacktivist "digital graffiti" campaigns that grabbed headlines but lacked coercive force**
- **State-sponsored strikes on banks, exchanges, and infrastructure as psychological signaling**
- **Information-control measures—blackouts and media blocks—that hurt civilians more than combatants**
- **Spyware operations targeting devices and communications for clandestine reconnaissance**
- **The persistent gap between cyber hype and battlefield reality, where no attack achieved a decisive edge**

The recent Israel–Iran war, while marked by large-scale military strikes and shifts in regional power, saw cyber operations that proved far less consequential than many expected. Both sides unleashed waves of hacktivist activity—over thirty-five pro-Iran groups and more than a hundred hacktivist collectives declared participation—defacing state television broadcasts with anti-regime footage and mounting DDoS campaigns that comprised roughly 40 percent of attacks on Israel. Yet these efforts functioned more as attention-grabbing "digital graffiti" than coercive blows: they shaped narratives in the information domain without degrading military or critical infrastructure capabilities.

State-sponsored offensives scored a handful of headlines—Predatory Sparrow's hacks of Iran's Bank Sepah, knocking essential banking services offline, and the assault on Nobitex that siphoned and "burned" about $90 million in cryptocurrency—but these strikes, like Iranian ransomware pushes by Pay2Key.IP or document dumps from Handala Hack accusing a London-based journalist of spying, mostly sowed chaos among civilians rather than delivering battlefield leverage. Their chief value lay in signaling: each side proved it could disrupt everyday life inside the other's borders, but neither breach translated into sustained operational advantage.

Meanwhile, efforts to control information flows imposed real hardship on ordinary citizens. Iran's near-total internet blackout on June 20 slashed national traffic by 97 percent under the guise of cybersecurity, and in Israel police briefly barred foreign outlets from reporting on missile strikes at select sites. These moves bought regime security by muffling criticism and obscuring battlefield realities, but they offered no enduring military benefit and inflicted broad social and economic pain.

The murkiest cyber front was spyware. Reports emerged of Israelis deploying commercial spyware—often from private firms with suspected state ties—to infiltrate Iranian devices both inside the country and abroad, even as Tehran accused WhatsApp of funneling user data to Israel (an allegation WhatsApp has denied). Israeli warnings that Iranian actors were hijacking home-security cameras to assess strike impacts added another layer of clandestine reconnaissance. Spyware's reward lies in the intelligence it yields, yet its gains are enabling rather than decisive, and overt deployment risks exposing tactics that states would prefer to keep hidden.

The 2010 Stuxnet operation remains the singular example of a decisive cyber strike—covertly degrading Iran's Natanz centrifuges and setting back its nuclear program for years. Crafting such specialized malware took nearly a decade and interagency collaboration, and deploying it permanently exposed a high-grade capability. That calculus explains why neither Israel nor Iran has unleashed a Stuxnet-style attack in this current conflict: the strategic value of surprise and denial outweighs short-term disruption.

In conclusion, together, these activities furnished only incremental edges—in reconnaissance, signaling, and information shaping—without tilting the military balance. High-grade destructive tools remain on ice, their development timelines and deterrent value too precious to squander. Instead, future cyber operations in this protracted rivalry will likely mirror what we saw here: low-level hacktivism, targeted espionage, and psychological signaling—all as adjuncts to kinetic force rather than war-winning instruments.

Reference **: What the Israel-Iran conflict revealed about wartime cyber operations-** *written by Nikita Shah in ATLANTIC COUNCIL*

(https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/)