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

MP-IDSA

Commentary

Cyber Operations in the Israel–US Conflict with Iran

Cherian Samuel

March 19, 2026

Summary

Cyberattacks have formed an important supporting component of the joint Israel–US campaign against Iran.

Cyberattacks have formed an important supporting component of the joint Israel–US campaign against Iran. However, the sheer intensity of the kinetic conflict has largely put these operations in the shade. As is increasingly the trend in modern conflict, cyber capabilities were employed to advance both tactical and strategic objectives in the early stages of the conflict.

Cyber operations play a critical role in shaping the battlefield, with actions designed to weaken the adversary's defences, morale and command capabilities before kinetic hostilities commence. The combined capabilities of the United States and Israel ensured that a range of such actions were undertaken even before the first bombs were dropped.

Senior US military officials stated that coordinated cyber and space activities degraded Iranian communications, sensors and command-and-control networks. According to Gen. Dan Caine, Chairman of the Joint Chiefs of Staff, "The first movers were USCYBERCOM and USSPACECOM, layering non-kinetic effects, disrupting and degrading and blinding Iran's ability to see, communicate and respond."[1] Secretary of War Pete Hegseth also alluded to "classified effects", which, in US military parlance, refers to the outcomes produced by an operation, not merely the tools employed, underscoring the emphasis on integrated effects across the cyber, space and kinetic domains.

Early Operational Effects and Infrastructure Disruption

On the second day of the conflict, the Israeli Defence Forces claimed in a statement that the headquarters of the IRGC's "cyber and electronic headquarters" and its "Intelligence Directorate" were destroyed in aerial strikes.[2] Monitoring organisations reported that Iran's internet connectivity dropped to about 4 per cent of normal levels due to multi-layered attacks on BGP routing, DNS infrastructure and SCADA/ICS systems, with some regions experiencing near-total blackouts.[3] Who was responsible for this was difficult to assess, as the Iranian government had itself imposed a blackout to prevent civil unrest, which was likely intensified by coordinated external cyber and military operations targeting Iranian communications infrastructure.[4]

[1] **"Secretary of War Pete Hegseth and Chairman of the Joint Chiefs of Staff Gen. Dan Caine Hold a Press Briefing [Transcript]"**, U.S. Department of War, 2 March 2026.

[2] **"Israel Targets Iran's Cyber Headquarters"**, *Politico*, 4 March 2026.

[3] **"Iran Internet Blackout Deepens, Disrupts Even State Media: Watchdog"**, *Arab Times* (Kuwait), 16 March 2026.

[4] **"Iran Networks Suffer Losses Amid Airstrikes, Showing Digital Evolution of Conflicts"**, *Fox News*, 1 March 2026.

Among the initial strategic objectives was the decapitation of the regime. In the early phase of the conflict, Trump's messaging implied that regime change or regime collapse in Iran could be a potential outcome of the war. Among the tactical steps undertaken in pursuit of this goal was targeting the entire regime leadership, including Ayatollah Khamenei.

According to reports, Israeli intelligence leveraged existing access to Tehran's traffic camera network and mobile phone infrastructure to trace the movements of the Iranian leadership with unprecedented precision.[5] In earlier reports, Israeli officials had said Iranian operators had broken into municipal traffic-camera networks and used the live feeds to assess missile-strike damage, track emergency-response movements, and identify whether specific targets had been successfully hit.[6] Such capabilities highlight the role of cyber access in enabling precision targeting, blurring the line between intelligence collection and operational execution.

Information Warfare and Psychological Operations

Coordinated cyberattacks simultaneously targeted Iranian digital infrastructure. Described in some reports as the "largest cyberattack in history", these operations disrupted government websites, mobile applications and online platforms through outages and defacements.[7] Following Israeli strikes on facilities of the state broadcaster IRIB, Israeli forces reportedly hijacked the broadcast feed to air political messages urging resistance against the Iranian government. Additional psychological operations included the compromise of a widely used Iranian prayer application, through which messages encouraging security personnel to defect were disseminated. These operations underscore the use of cyber capabilities not only for disruption but also for shaping perception and influencing behaviour.

Iran's Cyber Capabilities and Response

Over the years, Iran has significantly expanded its cyber warfare capabilities since the 2010 Stuxnet attack, widely believed to be a joint Israel–US operation that caused its nuclear centrifuges to spin out of control, evolving from limited DDoS and wiper malware to sophisticated state-sponsored cyber operations including large-scale

[5] Brijesh Singh, **"Inside the Code: Cyber Assassins"**, *The Sunday Guardian*, 8 March 2026.

[6] **"Iran Has Attacked Every Israeli Citizen Multiple Times, New Cyber Chief Yossi Karadi Says"**, *The Jerusalem Post*, 9 December 2025.

[7] **"Israel Plunges Iran Into Darkness With Largest Cyberattack in History During Attack Against Iran"**, *The Jerusalem Post*, 28 February 2026.

destructive attacks, espionage, supply chain attacks, and identity weaponisation with remote wipe commands affecting hundreds of thousands of devices. The Stuxnet attack served as a catalyst, or "awakening", prompting Iran to invest heavily in cyber capabilities, resulting in a 1,200 per cent increase in cybersecurity budgets in the years following the incident.[8]

Iran has developed advanced cyber capabilities distributed primarily across organisations such as the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS).[9] Iran has also built a large proxy hacking network outside the country, which has proved instrumental in carrying out attacks even after internet connectivity within Iran was severely degraded. This reliance on proxies reflects an adaptive approach to maintaining operational reach despite internal constraints.

Iran's immediate goal was to demonstrate its ability to retaliate asymmetrically. These attacks also needed to be visible and disruptive to influence public perception both domestically and internationally. According to the threat intelligence platform Falconfeeds, of the 72+ groups it tracked, 59 were pro-Iran and 11 anti-Iran, with varying degrees of sophistication depending on whether they were state-affiliated APTs, high-impact actors, or hacktivist collectives.[10]

Regional Spillover and Proxy Activity

From early March, these groups claimed to have carried out numerous operations, including a wave of DDoS disruptions against the Kuwaiti government and financial institutions such as the e-Government portal, and the ministries of Defence, Foreign Affairs, Health, Education, Finance, and Oil, as well as entities like Burgan Bank and the Kuwait News Agency.[11]

Known Israeli sites targeted by DDoS included the Movement for Freedom of Information (meida.org.il) and RAN Investment House, reflecting ongoing low-level cyber harassment in the Iran–Israel shadow conflict.[12] Jordanian websites also saw

[8] Ashish Sen, **"Iran's Growing Cyber Capabilities in a Post-Stuxnet Era"**, The Atlantic Council, 10 April 2015.

[9] **"Iran's Cyber Playbook in the Escalating Regional Conflict - Rapid7"**, Rapid7, 12 March 2026.

[10] **"Inside Middle East Cyber Shadow War: Pro-Iran & Anti-Iran Threat Actor Mapping"**, FalconFeeds, 4 March 2026.

[11] FalconFeeds, **"Hider Nex targets Kuwaiti government and financial websites..."**, X (formerly Twitter), 11 March 2026.

[12] FalconFeeds, **"Conquerors Electronic Army claims to have targeted the website of The Movement for Freedom of Information..."**, X (formerly Twitter), 15 March 2026.

over 69 claimed incidents across more than 40 targets, including government ministries, banks, airports, energy firms and ICS-related systems.

Bahrain experienced repeated targeting, reflecting its status as a Gulf state that hosts US naval assets, with multiple waves of DDoS attacks hitting government ministries and financial institutions. Qatar also reportedly faced significant DDoS traffic against government and critical services, including the Amiri Diwan, Ministry of Interior e-services, and the national e-government portal.[13]

Taken together, these operations reflect a pattern of distributed, low-intensity cyber activity aimed at signalling capability. This could also mean that more disruptive options are being reserved for later stages of the conflict.

High-Value Targets and Blended Threats

While most of these incidents qualified as low-level cyberattacks without large-scale or enduring damage, several "high-value soft targets"—such as undersea cables, internet exchange points, cloud infrastructure and global navigation systems—could be subject to kinetic attacks, and in some cases already were. Amazon's Bahrain data centre site was reportedly taken offline following nearby drone strikes, while two additional AWS-related sites in the UAE were directly hit. Iran justified the strike by accusing Amazon of supporting US military and intelligence activity through its data centres.[14] In the United States, too, critical infrastructure, from financial services to water utilities, to transportation infrastructure, has been the target of Iranian actors before and could well come under attack again after they regroup and as the kinetic conflict intensifies.[15]

The Stryker Cyberattack

The most notable event so far has been a major cyberattack against US medical technology giant Stryker on 11 March, which resulted in global system outages and widespread operational disruption. Stryker, a US$ 134 billion company specialising in orthopaedics, MedSurg, neurotechnology and hospital systems, employs more than 50,000 people worldwide, including over 2,000 in India working in R&D.

[13] FalconFeeds, **"Hider_Nex claims to have targeted multiple websites in Bahrain..."**, X (formerly Twitter), 9 March 2026.

[14] **"Amazon Bahrain Data Centers Targeted in Iran Drone Strike"**, *CNBC*, 4 March 2026.

[15] **"How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?"**, Center for Strategic & International Studies (CSIS), 3 March 2026.

The outage was global, with employees locked out of systems that were reportedly wiped. In successive updates on its customer service page, the company noted that the breach took place within its internal Microsoft environment.[16] It took the company over four days to recover, while its share price fell by 9 per cent, resulting in an estimated US$ 6–8 billion loss in market capitalisation.

A pro-Iran hacktivist group calling itself Handala, with links to Iran's Ministry of Intelligence and Security (MOIS), alleged that it had remotely wiped over 200,000 systems and stolen 50 terabytes of data. The group claimed the attack was in retaliation for a February missile strike that hit an Iranian school and killed at least 175 people, most of them children. [17]

Incidents such as the Stryker cyberattack demonstrate that while cyber operations may be secondary in strictly military terms, they can generate significant economic and societal disruption, particularly when targeting private-sector entities embedded in global supply chains.

The relatively limited impact of the cyber operations so far suggests that, in a kinetic war, less emphasis is placed on cyber effects once infrastructure is physically degraded. Kinetic attacks tend to produce more immediate and lasting damage, while cyber effects are often temporary.

Overall, cyber capabilities function less as decisive instruments of war and more as force multipliers that shape, support and exploit the effects of kinetic operations.

While not decisive on their own, they have been integral in preparing the battlefield and enabling these effects. At the same time, the relatively limited impact observed may reflect not only structural constraints—such as dependence on connectivity—but also a degree of strategic restraint, with more disruptive capabilities potentially held in reserve for escalation.

[16] **"A Message to Our Customers"**, Stryker, March 2026.

[17] **"Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker"**, *Security Boulevard*, March 2026.

About the Author

Dr. Cherian Samuel is Research Fellow 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