Iran’s Cyber Playbook in the Escalating Regional Conflict

By Rapid7

Published: 2026-03-11 · Archived: 2026-04-05 15:57:50 UTC

Following our recent published advisories, this publication is intended to outline a summary of the cyber activities associated with the tension. Based on the available information, we believe the conflict is beginning to show signs of expanding beyond a strictly regional crisis. Initial threat reporting pointed to a measurable increase in cyber activity linked to the crisis predominantly focused on hacktivist mobilization, with reports of phishing campaigns, and claims of data theft and disruptive operations. For a companion piece focused around our customers, dive into ***Rapid7 Detection Coverage for Iran-Linked Cyber Activity***.

Cyber activity by groups associated with Iran and their affiliated ecosystems have begun to surface. Much of the visible activity currently appears to have limited immediate operational impact as it consists primarily of website defacements, distributed denial-of-service (DDoS) attacks, coordinated messaging campaigns, phishing attempts, and reconnaissance against exposed digital infrastructure. While these incidents may appear opportunistic or symbolic, historical patterns of such behavior suggest that this activity can represent early-stage signaling, pressure, and preparatory shaping operations rather than isolated disruption.

Iran’s cyber ecosystem operates through a layered structure that includes state-linked advanced persistent threat (APT) groups, proxy actors, hacktivist personas, and sympathetic foreign collectives. Even when not centrally coordinated, these actors often converge on the same narratives and target sets during geopolitical crises, enabling simultaneous visible disruption and covert intelligence-driven intrusion activity. As the conflict evolves, this ecosystem provides a scalable and deniable tool for retaliation that can gradually intensify.

It is very likely that the cyber risk will widen accordingly as the current conflict continues. Governments and organizations located in regions hosting U.S. military infrastructure or closely aligned with U.S. and Israeli positions may face increased exposure, particularly across sectors such as logistics, critical infrastructure, public administration, energy, and telecommunications.

Strategic context and operational trends

Iran does not operate according to a single publicly articulated cyberwarfare doctrine. Instead, its cyber strategy has evolved pragmatically as part of the country’s broader asymmetric security model. Since 2010, there has been an expansion of its cyber capabilities as instruments for intelligence gathering, internal control, retaliation, coercive messaging, and regional influence. Cyber operations are therefore best understood not as a separate military domain with a fully transparent doctrine, but as an adaptable component of the regime’s survival and strategic competition against outsiders.

Broadly speaking, Iranian cyber activity tends to serve three overlapping strategic objectives. The first is regime security and domestic control, in which cyber tools support surveillance, information control, and disruption of dissident or opposition networks. The second is strategic intelligence collection, in which state-linked actors target

governments, defense organizations, technology providers, telecommunications firms, and critical infrastructure to gather political, military, and economic intelligence. The third is coercive signaling and regional influence, in which cyber operations impose costs on adversaries, shape perceptions, and demonstrate retaliatory capability while remaining below the threshold of overt interstate war.

A key feature of this regime's approach is the development of long-term access. Iranian APT groups often conduct sustained intrusion campaigns focused not only on immediate collection but also on access persistence, credential harvesting, and network familiarity. In a crisis environment, these pre-existing footholds can become strategically important, supporting either intelligence collection or later disruptive operations. This is one reason current low-visibility intrusions deserve as much analytical attention as public hacktivist claims. The visible DDoS or defacement campaign may dominate headlines, but the more significant strategic risk often lies in covert access established inside other targets.

Another defining feature of Iran's cyber strategy is its layered operational model. State-linked APT groups frequently operate alongside contractors, proxies, persona-driven influence actors, and hacktivist collectives. This structure offers several advantages: it creates deniability, increases operational tempo; broadens the range of possible targets; and allows Iran-aligned ecosystems to combine disruptive spectacle with intelligence-driven depth. During periods of heightened tension, this blended model enables visible pressure operations to coexist with quieter espionage or pre-positioning campaigns. Current reporting on the conflict strongly supports this interpretation, with activist and proxy campaigns surging in parallel to concern over state-linked phishing, malware, wipers, and infrastructure-focused targeting.

Iran's threat actor landscape

State sponsored

Iran's cyber capabilities are distributed across a hybrid ecosystem of state institutions, intelligence services, military structures, and semi-official operators. Rather than relying on a single centralized cyber command, Tehran appears to allocate responsibilities across different organs, primarily the Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security, with support from contractors, front entities, and affiliated personas. Strategic coordination of the cyber domain is overseen by the Supreme Council of Cyberspace, while operational activities are carried out through a mix of official and semi-official channels.

IRGC-linked actors

The **Islamic Revolution Guard Corp** (IRGC) maintains one of Iran's most visible offensive cyber capabilities and has been associated with cyber espionage, influence operations, credential theft, and politically aligned disruptive activity. Among the principal IRGC-linked actors are **APT35** (also known as Charming Kitten or Mint Sandstorm), which has long conducted spear-phishing and credential-harvesting operations against diplomats, journalists, researchers, and policy communities; **APT42** is an actor particularly associated with surveillance and social engineering targeting dissidents, activists, journalists, and policy experts. **Cotton Sandstorm** (also known as Holy Souls and Emennet Pasargad), meanwhile, has been linked to both espionage and influence-oriented operations targeting regional adversaries and Western institutions. Recent reporting also highlights continued

concern around malware associated with this broader actor set, including infostealing and espionage tooling used in phishing-led operations.

MOIS-linked actors

The Ministry of Intelligence and Security (**MOIS)** operates parallel cyber capabilities that tend to emphasize intelligence collection, long-term access, and strategic espionage. The most prominent groups in this cluster include **MuddyWater** and **OilRig** (also known as APT34). CISA has previously described MuddyWater as an Iranian government-sponsored actor conducting cyber espionage and malicious cyber operations across multiple sectors, while current reporting continues to place the group among the most operationally relevant Iranian state-linked threats in the present crisis environment. OilRig remains a longstanding espionage actor focused on governments, financial institutions, energy entities, and other strategic organizations.

These actors illustrate Iran's distributed cyber-operational model: Intelligence-driven access development, influence, psychological pressure, and opportunistic disruptive action are not separate lines of effort but parts of a broader strategic continuum.

Parallel hacktivist and proxies

Beginning in June 2025, a noticeable surge in hacktivist and proxy cyber activity accompanied the broader escalation of tensions in the Middle East. This reflects a recurring pattern observed during previous geopolitical crises, in which ideologically aligned non-state cyber actors mobilize alongside, or in parallel with, state-linked cyber operations. In the current confrontation, this dynamic has again expanded the cyber landscape beyond traditional state-directed espionage or sabotage.

By early March 2026, several dozen hacktivists or proxy collectives emerged related to the conflict. These groups vary significantly in capability and reliability. Some focus on distributed denial-of-service (DDoS) attacks, while others conduct website defacements or hack-and-leak campaigns. Some primarily amplify claims of compromise that are exaggerated or only partially verifiable. Their significance, therefore, lies less in technical sophistication than in the cumulative pressure they place on defenders and the broader information environment.

In crisis situations, this activity can produce strategic effects. Numerous low-impact incidents can consume defensive resources, complicate attribution, and obscure more sophisticated intrusions occurring simultaneously. Hacktivist campaigns may therefore function as distractions, signals, or psychological pressure while more capable actors pursue quieter access to high-value networks. For this reason, the analytical distinction between advanced persistent threat (APT) activity and hacktivism can become blurred during periods of geopolitical confrontation.

Several collectives active in the current environment publicly position themselves as ideologically aligned with Iran or with members of the so-called "Axis of Resistance." Among the more visible groups are Handala Hack Team, Dienet, FAD Team, APT IRAN, Cyber Islamic Resistance, and Fatimion cyber team. These actors frequently frame their operations as retaliatory cyber campaigns targeting Israeli, Western, or allied regional entities, claiming responsibility for activities such as website defacements, DDoS attacks, and hack-and-leak operations targeting mainly government, telecommunications, energy, and financial entities. Although many

claims remain difficult to verify independently, their messaging strategy often emphasizes their psychological and reputational impact.

In parallel, several pro-Russia hacktivist groups have also engaged in operations linked to the confrontation, including NoName057(16), Sever Killer, and Russian Legion. These groups typically conduct large-scale DDoS campaigns targeting government portals, financial services, and transportation or telecommunications infrastructure in states perceived as supporting Israel or broader Western policy positions. Their participation illustrates how regional conflicts can attract cyber actors from outside the immediate theater when ideological alignment or strategic narratives converge.

Cyber activities linked to the ongoing conflict

Iranian APT group operations

Beyond the highly visible hacktivist activity circulating on social media, defacement platforms, and Telegram channels, a quieter but more strategically significant layer of cyber operations is unfolding through Iranian state-linked APT groups. These operations appear ongoing and aligned with broader geopolitical objectives tied to the current conflict environment.

Recent threat reporting indicates continued operations by the Iranian APT group, MuddyWater, which is widely assessed to be linked to MOIS. Since at least early February 2026, reporting has suggested potential compromises or attempted intrusions targeting organizations associated with the United States and allied interests.

According to public reporting, activity linked to the group was reportedly observed within the networks of a United States–based bank, a United States airport, a nonprofit organization operating across the United States and Canada, and a software company with operations in Israel. In several of these incidents, threat actors reportedly deployed a previously undocumented backdoor known as Dindoor, suggesting a coordinated, ongoing campaign rather than isolated compromise events.

Hacktivist and proxy disruption activities

The most visible form of cyber activity so far remains hacktivist and proxy-led disruption.

DDoS attacks are among the most common tactics employed by hacktivist groups. Pro-Russia groups such as NoName057(16) and Server Killers, along with other pro-Iran collectives affiliated with them, have been linked to waves of coordinated DDoS attacks against Israel, Qatar, Bahrain, and other politically symbolic targets. These attacks are generally inexpensive and cause only short-term technical damage, but they remain strategically useful because they disrupt public services, tie up defense resources, generate media coverage, and fuel the narrative of a sustained cyber response.

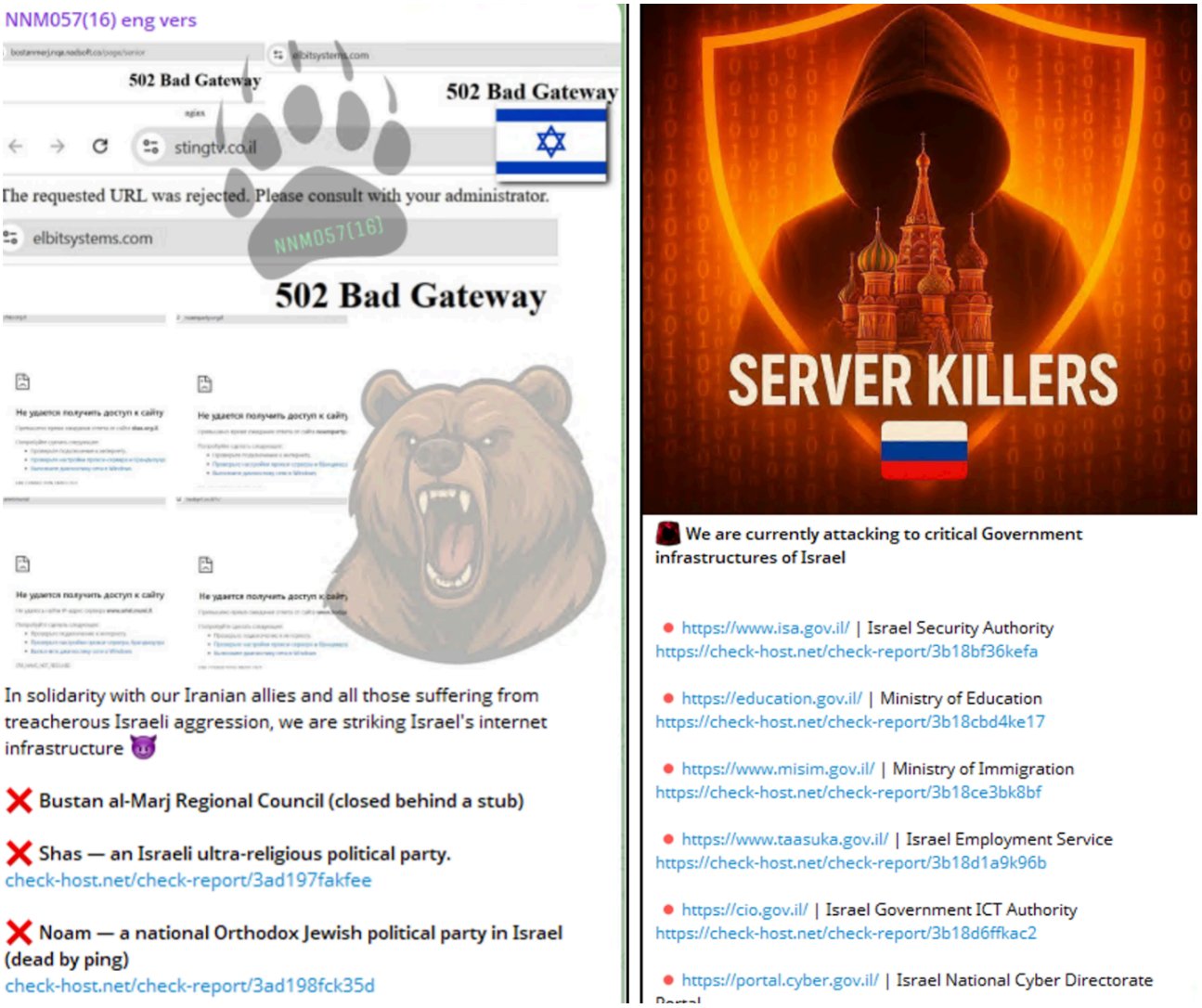

Figure 1: Telegram post from pro-Russia hacktivist groups claiming responsibility for targeting an Israeli website in support of Iran

Website defacement also remains a common tactic. Groups such as FAD Team, 313, and Cyber Islamic Resistance have been associated with claims of attacks on several websites. Although defacements are technically simple to execute, they remain analytically significant: They are highly visible, rapidly disseminated, and psychologically impactful, often creating an exaggerated perception of widespread systemic compromise.

Data breaches represent a far more significant dimension of cyber operations. The Iranian-aligned group Handala, in particular, continues to blend political messaging with claims of data theft and the selective release of allegedly compromised information. The group recently asserted that it had infiltrated a Saudi energy company and exfiltrated internal documents, framing the operation as a combination of data exfiltration, coercive pressure, and psychological warfare targeting the energy sector. Even when the full authenticity of released datasets cannot be independently verified, the publication of partially credible material can still generate substantial reputational damage and potential operational disruption for affected organizations.

Targeting critical infrastructure has emerged as one of the most concerning aspects of the current cyber activity by pro-Iran hacktivists and proxy collectives. Groups operating in this ecosystem, including Iranian APTs, Handala, and networks associated with the Cyber Islamic Resistance umbrella, have publicly claimed operations targeting infrastructure across the region. Recent Telegram posts indicate that an Iranian APT group claimed responsibility for attempts to sabotage Jordanian critical infrastructure, while other Iran-aligned hacktivist personas have asserted access to sectors including fuel systems, water utilities, and other operational technology environments.

In a separate case, the Handala Hack Team has alleged that it compromised both Oil and gas companies in the United Arab Emirates and Israel, claiming to have exfiltrated more than 1.3 TB of sensitive data from oil and gas sector networks. These claims, which would represent a significant intrusion into Middle Eastern energy infrastructure if confirmed, have circulated primarily through hacktivist communication channels and social media reporting and have not been independently verified.

Figure 2: IRAN APT group claimed attempts to target Jordanian critical infrastructure

Although many of these claims remain difficult to independently verify, the recurring focus on industrial control systems and essential services is analytically significant. Hacktivist collectives aligned with Iranian geopolitical narratives frequently leverage infrastructure-related claims as part of information operations designed to amplify perceived impact, generate psychological pressure, and signal the potential for escalation into operational technology environments. Even when technical disruption is limited or exaggerated, the persistent narrative around infrastructure compromise can shape defensive priorities and highlight potential escalation pathways within the broader cyber conflict.

Sectoral exposure and risk landscape

In the current geopolitical context, cyberattacks extend far beyond military networks and defense institutions. Modern cyber operations increasingly aim to affect the broader ecosystem that supports government activity, economic stability, and public trust. Consequently, adversaries seek not only technically vulnerable targets but also organizations whose compromise or disruption can increase visibility, influence public perception, or create cascading effects across interconnected systems.

A successful intrusion into a widely used service provider, a major infrastructure operator, or a publicly accessible institution can quickly produce consequences that extend far beyond the initial target, affecting supply chains, service availability, and public confidence. In this context, cyber operations often serve multiple purposes simultaneously: intelligence gathering, strategic positioning within critical networks, and generating disruption or exerting influence during periods of heightened geopolitical tension.

At present, several sectors appear particularly exposed:

- Government institutions and public administration
- Defense and aerospace industry
- Energy sector, including oil, gas, and electricity
- Telecommunications providers
- Financial services
- Transportation systems

However, the risk landscape extends beyond these sectors themselves. Organizations that form part of the broader digital supply chain supporting these industries may also represent attractive entry points. This includes cloud service providers, managed service providers, technology vendors, and other third-party platforms that maintain privileged access to client environments. Compromising such intermediaries can allow adversaries to reach high-value targets indirectly. By gaining access to a supplier or service provider, attackers may obtain pathways into multiple networks simultaneously, access sensitive information, or move laterally across interconnected operational systems. Supply chain compromise, therefore, offers both scale and stealth, making it an increasingly common tactic in sophisticated cyber campaigns.

Geopolitical alignment can also influence targeting decisions. Organizations based in countries that host United States military assets or are publicly aligned with United States or Israeli policy positions may attract additional attention from adversaries. In these cases, targeting can carry symbolic, political, or strategic value beyond the immediate technical impact of the intrusion. Within this environment, cyber exposure can generally be understood through three overlapping targeting dynamics.

Symbolic targets include municipalities, universities, media outlets, and public institutions. These organizations may be targeted primarily for visibility, messaging, or propaganda purposes. Even limited disruption or data exposure can generate headlines and amplify the perceived reach of the attackers.

Operational targets include sectors that support everyday economic and social activity, such as telecommunications providers, transportation systems, payment networks, and fuel distribution infrastructure. Disruptions in these areas can quickly affect daily life, creating public anxiety and increasing pressure on authorities to respond.

Strategic targets consist of entities whose compromise offers long-term intelligence or operational value. This category includes defense contractors, major financial institutions, government networks, and operators of critical infrastructure. In these cases, adversaries may prioritize persistence and stealth to collect intelligence, monitor decision-making processes, or maintain access that could be leveraged during future crises.

Taken together, these targeting patterns illustrate a broader shift in cyber operations: Attackers are increasingly selecting targets not only for their intrinsic value, but for the broader political, economic, and societal effects that disruption or compromise can produce.

What should organizations monitor?

In the current phase of the conflict, organizations should continue to monitor for indicators that activity is shifting from opportunistic disruption toward deliberate intrusion or access preparation.

Internet-facing infrastructure is often the initial entry point. Elevated scanning or probing of public websites, VPN gateways, remote access portals, cloud services, and email authentication infrastructure may indicate early reconnaissance. While some scanning is routine, sudden increases in probing activity or authentication attempts should be treated as potential precursors to intrusion.

Phishing and social engineering campaigns are also likely to intensify. Threat actors may exploit developments in the conflict by using lures that reference civil defense alerts, battlefield updates, humanitarian messaging, or urgent requests that appear to originate from leadership or trusted partners. In some cases, malicious applications or replicas of legitimate services may be used to harvest credentials or deploy malware.

Credential misuse remains a primary access vector. Security teams should monitor for abnormal authentication patterns, including logins from unusual geographic locations, access at unexpected hours, repeated failed logins followed by success, changes to multi-factor authentication settings, or the creation of new privileged accounts.

Organizations operating critical infrastructure should closely monitor activities within their operational environments. Suspicious access to remote management platforms, unusual connectivity between IT and OT networks, or unexpected activity involving engineering workstations or vendor access channels may signal reconnaissance within sensitive systems.

Finally, monitoring the broader information environment can provide early warning and signal the need to increase monitoring. Hacktivist groups frequently use platforms such as Telegram and X to circulate target lists, claim attacks, or release fragments of allegedly stolen data tied to geopolitical events. Tracking these channels can help organizations identify potential targets and strengthen their defensive posture before malicious activity reaches their networks.

Additional reading from Rapid7 Labs, for Rapid7 customers: ***Rapid7 Detection Coverage for Iran-Linked Cyber Activity***

Source: https://www.rapid7.com/blog/post/tr-iran-cyber-playbook-escalating-regional-conflict/