

IRAN'S HYBRID CYBER WARFARE ECOSYSTEM

From Espionage and Influence Operations to Proxy Hacktivism Against Israel, the United States, and Middle Eastern Countries



July 2026

By Jeremy Makowski

Cyber Threat Intelligence Expert (Crime, Warfare and Counter Terrorism)

Table of Contents

Disclaimer **4**
Methodology and Confidence Levels **5**
Executive Summary **6**
Key Judgments **8**
1. Strategic Context **9**
1.1 Iran’s Geopolitical Environment 9
1.2 Cyber as an Instrument of National Power 10
1.3 Strategic Objectives 11
Regime Survival and Deterrence 11
Intelligence Collection 12
Retaliation and Escalation Management 12
Suppression of Dissent 12
Psychological and Information Operations 12
1.4 Hybrid Conflict, Decentralization, and Operational Resilience 13
1.5 Evolution of Iranian Cyber Strategy 15
2. Understanding Iran's Cyber Power **18**
2.1 Strategic Leadership and Decision-Making 18
2.2 The IRGC and MOIS Cyber Architecture 19
2.3 Universities, Contractors, and the Innovation Ecosystem 21
2.4 Proxy, Criminal, and Hacktivist Networks 22
2.5 International Military and Cyber Partnerships and Support 25
2.5.1 Military Cooperation 25
2.5.2 Cyber Cooperation 29
3. The Iranian Operational Model **32**
3.1 How Iran Builds Cyber Operations 32
3.2 Intelligence Collection and Target Development 32
3.3 Operational Tradecraft 33
3.4 Cyber Espionage Operations 34
3.5 Influence and Psychological Operations 38
3.6 Disruptive and Destructive Operations 40
3.7 Integration with Military, Proxy, and Information Operations 40
4. Strategic Targeting **41**
4.1 Israel 41
4.2 The United States and Western Allies 42
4.3 Gulf States and Regional Adversaries 42
4.4 Critical Infrastructure and Strategic Industries 43
4.5 Dissidents, Opposition Networks and Civil Society 43
5. Iran Under Cyber Pressure **44**
5.1 Major Operations Against Iran 44

5.2 What Those Operations Revealed 45
5.3 Iranian Defensive Adaptation 45
5.4 Intelligence Opportunities 46
6. Strategic Assessment **50**
6.1 Strengths of the Iranian Cyber Model 50
6.2 Structural Weaknesses 50
6.3 Intelligence Gaps 51
6.4 Indicators of Strategic Change 51
6.5 Future Outlook 52
Conclusion **53**
About the Author **54**
References **55**

Disclaimer

This report is made freely available for informational, educational, and research purposes. It is intended to support a deeper understanding of the evolving Iranian cyber conflict ecosystem and does not constitute legal, operational, financial, or security advice.

The report is based primarily on publicly available information. Although every effort has been made to ensure accuracy, some information concerning ongoing cyber, intelligence, and military operations may remain incomplete, contested, or subject to revision.

Any reproduction, quotation, adaptation, or distribution of this report, whether in whole or in part, must include appropriate attribution to the author and a clear reference to the original publication.

Commercial use, resale, or incorporation of this report into a commercial product or service is prohibited without the author's prior written consent.

Methodology and Confidence Levels

This report draws on publicly available government statements, cybersecurity advisories, threat-intelligence reporting, sanctions designations, judicial documents, investigative journalism, academic research, corporate records, technical analysis, and other open-source intelligence.

Information concerning ongoing military, intelligence, and cyber operations may be incomplete, contested, deliberately manipulated, or subject to revision. The report therefore distinguishes among the following categories of information:

- Officially confirmed information
- Information corroborated by multiple independent and credible sources
- Analytical assessments derived from observable indicators
- Claims that remain unverified, disputed, or insufficiently substantiated

The following confidence terminology is used throughout the report:

High confidence indicates that an assessment is supported by multiple reliable and independent sources, authoritative technical evidence, official documentation, or a consistent body of corroborated reporting.

Moderate confidence indicates that an assessment is credible and supported by available evidence, but that significant intelligence gaps, attribution uncertainties, or plausible alternative explanations remain.

Low confidence indicates that an assessment relies primarily on limited, indirect, secondary, disputed, or potentially manipulated reporting.

Confidence levels reflect the quality, reliability, and consistency of the available evidence rather than the potential severity of the assessed threat. They should be reviewed and, where necessary, revised as new information becomes available.

Executive Summary

Iran's cyber capabilities have entered a new phase of development. Recent military pressure, leadership losses, economic constraints, and regional setbacks have weakened important elements of Tehran's conventional and proxy-based deterrence posture. They have, however, not eliminated Iran's capacity to conduct cyber operations. Instead, these pressures appear to be accelerating the evolution of a more decentralized, resilient, and deniable cyber ecosystem built around state institutions, contractors, front companies, proxy organizations, hacktivist personas, criminal intermediaries, and distributed operational infrastructure.

This report argues that Iranian cyber power should be understood as an interconnected operational ecosystem rather than as a collection of isolated Advanced Persistent Threat groups. The Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security remain the principal strategic institutions associated with Iranian offensive cyber activity. Increasingly, however, their role extends beyond direct operational execution to include strategic tasking, financing, access management, contractor supervision, capability development, and coordination across a wider network of affiliated actors.

Operational capacity is distributed across government organizations, universities, technical institutes, private contractors, front companies, ideologically aligned cyber personas, criminally motivated operators, and regional proxy networks. This distribution complicates attribution and allows parts of the system to continue operating even when individual commanders, infrastructure, organizations, or operational teams are disrupted.

Recent geopolitical escalation provides an important illustration of this model. Open-source reporting indicates that military strikes and connectivity disruption affected elements of Iran's centralized cyber leadership and command infrastructure. Nevertheless, proxy-linked, contractor-associated, and hacktivist activity continued or resumed rapidly. This pattern is consistent with a system that relies on pre-positioned access, delegated authority, standing contingency plans, distributed infrastructure, and varying degrees of operational autonomy. It does not, by itself, prove that all observed activity was centrally directed.

Iranian cyber operations must also be assessed within the broader context of Tehran's national security doctrine. Cyber capabilities operate alongside military force, intelligence collection, proxy warfare, sanctions evasion, economic coercion, influence operations, domestic repression, and diplomatic signaling. They are used not only to collect intelligence or disrupt systems, but also to support military campaigns, shape public perception, expose or intimidate individuals, suppress opposition networks, reinforce strategic narratives, and impose political and psychological costs on adversaries.

Relative to the more centralized military-intelligence structures often associated with Russia and the large-scale strategic collection model commonly associated with China, Iran places comparatively greater emphasis on operational adaptability, asymmetric cost imposition, deniable personas, political signaling, and the integration of technical activity with influence operations. These distinctions are relative rather than absolute, as all three states use combinations of government units, contractors, intermediaries, front organizations, and covert infrastructure.

Iranian campaigns frequently combine espionage, credential theft, social engineering, hack-and-leak operations, disruptive activity, ransomware-like behavior, influence operations, and exaggerated or fabricated claims. The purpose is often to maximize political and psychological impact while preserving ambiguity and limiting the likelihood of direct military retaliation.

The report examines the institutional architecture supporting this model, including the roles of the IRGC, MOIS, military cyber organizations, universities, private contractors, financial networks, cryptocurrency-enabled sanctions evasion, and international relationships involving Russia, China, North Korea, and regional proxy organizations. Together, these components form an adaptive ecosystem capable of regenerating at least part of its operational capacity despite sustained external pressure.

For governments, intelligence services, and critical-infrastructure operators, the principal implication is that military success against Iranian command structures should not automatically be interpreted as a proportional reduction in cyber risk. Leadership losses and infrastructure degradation may temporarily reduce coordination, operational tempo, or technical sophistication. They do not necessarily eliminate previously established access, delegated operators, contractor capability, proxy infrastructure, or the political incentive to retaliate.

Periods immediately following military escalation may therefore create both heightened risk and valuable intelligence opportunities. Defensive organizations should prioritize the identification of dormant access, compromised identities, exposed operational technology, third-party dependencies, and infrastructure that could be activated during a crisis.

Iran is unlikely to abandon cyber operations as an instrument of national power. As its conventional freedom of action becomes more constrained, cyber capabilities are likely to assume greater importance in intelligence collection, retaliation, coercive signaling, influence activity, sanctions evasion, and support to proxy networks.

Iran’s principal cyber strength does not lie in any single organization, malware family, or threat group. It lies in the resilience, adaptability, ambiguity, and strategic integration of an ecosystem designed to operate under conditions of prolonged military, economic, political, and technological pressure.

Key Judgments

- It is assessed with high confidence that Iran's cyber ecosystem has evolved into a distributed operational model capable of sustaining at least part of its offensive activity despite leadership losses, infrastructure disruption, and military pressure.

- It is assessed with high confidence that Tehran relies extensively on contractors, front companies, proxy actors, hacktivist personas, and criminally motivated operators to expand operational reach and preserve varying degrees of plausible deniability.

- It is assessed with moderate confidence that recent military strikes degraded elements of centralized command, coordination, and connectivity, but did not eliminate Iran's capacity to conduct cyber espionage, influence operations, disruptive activity, or proxy-enabled campaigns.

- It is assessed with high confidence that pre-positioned access within foreign networks represents one of Iran's most strategically valuable cyber assets during periods of geopolitical escalation.

- It is assessed with high confidence that a substantial proportion of pro-Iranian hacktivist claims are exaggerated, recycled, misleading, or unverifiable. Analysts should therefore distinguish among claimed activity, confirmed compromise, verified operational impact, and demonstrated state direction.

- It is assessed with high confidence that cyber operations are an integral component of Iran's broader hybrid warfare doctrine and should be analyzed alongside military activity, proxy mobilization, intelligence operations, sanctions pressure, and influence campaigns.

- It is assessed with moderate confidence that future Iranian cyber activity will place greater emphasis on resilience, delegated execution, identity compromise, psychological impact, strategic persistence, and proxy-enabled operations rather than on technical sophistication alone.

- It is assessed with moderate confidence that leadership decapitation may reduce short-term coordination and operational coherence while simultaneously increasing the relative autonomy, inconsistency, and unpredictability of contractor and proxy activity.

1. Strategic Context

1.1 Iran's Geopolitical Environment

Iran enters the current period from a position of significantly greater strategic weakness than it occupied two years earlier. A series of geopolitical developments beginning in late 2024 reshaped Tehran's regional environment and reduced its freedom of action. The collapse of Bashar al-Assad's government in Syria in December 2024 disrupted Iran's principal logistical corridor to Hezbollah and weakened one of its most important strategic anchors in the Levant. This erosion of regional depth complicated Tehran's ability to sustain proxy forces and maintain influence across Syria and Lebanon.

Pressure intensified in 2025, when the United States reinstated an expanded maximum-pressure policy combining additional sanctions, stronger secondary-sanctions enforcement, and a more confrontational posture toward the Iranian government. These measures further constrained Iran's economic room for maneuver and increased pressure on state institutions, defense-industrial networks, procurement channels, and sanctions-evasion mechanisms.

The strategic environment changed even more dramatically on February 28, 2026, when the United States and Israel launched a large-scale military campaign against Iran, designated Operation Epic Fury by the United States and Operation Roaring Lion by Israel. The opening strikes killed Supreme Leader Ali Khamenei and several senior Iranian military, intelligence, and security officials, while targeting nuclear, missile, air-defense, command, intelligence, cyber, and support infrastructure.

The campaign quickly developed into a sustained regional conflict. Iran responded with missile and drone attacks against Israel, U.S. military positions, Gulf states, and maritime targets, while the fighting expanded through Hezbollah and the Lebanese theater. The conflict also disrupted regional aviation, energy markets, commercial shipping, and access through the Strait of Hormuz, demonstrating the extent to which the confrontation had moved beyond a limited exchange of strikes.

A temporary ceasefire arrangement took effect in early April 2026, although implementation remained uneven and fighting continued in parts of the wider regional theater. On June 17, 2026, the United States and Iran signed an interim memorandum of understanding at Versailles intended to extend the ceasefire, support negotiations toward a longer-term settlement, and restore maritime access through the Strait of Hormuz. The agreement did not constitute a comprehensive peace settlement. By early July, renewed maritime incidents, mutual accusations of ceasefire violations, and a resumption of U.S. and Iranian military strikes had effectively undermined the framework, demonstrating the continued volatility of the conflict.

These events fundamentally altered the context in which Iranian cyber power must be assessed. The death of the Supreme Leader and the loss of significant elements of Iran's senior security leadership represented far more than the temporary degradation of a cyber command structure. They disrupted the wider political and national-security hierarchy through which cyber operations were authorized, coordinated, financed, and integrated with military, intelligence, proxy, and influence activity.

Open-source reporting differs regarding the precise timing, sequencing, targeting, and operational effects of individual strikes. Accordingly, unless a specific target or consequence is supported by authoritative reporting, this report refers to the broader February–April 2026 conflict rather than attributing particular effects to a single operation or date.

Despite this level of strategic disruption, available assessments suggest that the Iranian system is seeking to consolidate authority rather than approaching immediate collapse. A more hard-line governing structure backed by the Islamic Revolutionary Guard Corps and domestic security institutions would be likely to rely increasingly on deniable, asymmetric, and comparatively low-cost instruments of national power.

This is particularly relevant in the cyber domain. As Iran's conventional, regional, and economic options become more constrained, cyber operations are likely to assume greater importance as tools for intelligence collection, retaliation, coercive signaling, support to proxy networks, influence activity, and the imposition of political and psychological costs. The continuation of Iranian-linked cyber, contractor, proxy, and hacktivist activity despite the loss of senior leadership therefore provides an important test of the resilience and decentralization described throughout this report.

1.2 Cyber as an Instrument of National Power

Iran has long maintained a layered national-security system designed to preserve domestic control while projecting asymmetric power abroad. Within this system, the Islamic Revolutionary Guard Corps has evolved beyond its traditional military function into a major political, intelligence, economic, security, and cyber actor.

The 2010 Stuxnet operation against the Natanz nuclear facility represented a major strategic turning point. It demonstrated that cyber operations could generate physical effects against critical national infrastructure. For Iranian decision-makers, the incident highlighted both the country's vulnerability to offensive cyber operations and the strategic value of developing comparable capabilities.

Iran subsequently invested in both defensive and offensive cyber capacity. These capabilities were developed through formal state institutions, military and intelligence organizations, universities, technical institutes, private contractors, front companies, and aligned non-state actors.

This institutional model depends heavily on a parallel ecosystem of nominally private contractors, technical organizations, academic networks, and front companies that can obscure direct government attribution. Entities such as Emennet Pasargad and the Rana Intelligence Computing Company have been linked through government designations, judicial documents, and threat-intelligence reporting to Iranian state-directed or state-supported activity.

By operating through such organizations, Tehran can combine civilian technical expertise with national-security requirements while maintaining organizational ambiguity. This model can lower the political and operational cost of espionage, infrastructure targeting, information theft, influence operations, and disruptive activity.

Iran's cyber strategy emphasizes asymmetric cost imposition. Its operations often seek to generate psychological pressure, consume defensive resources, damage public confidence, and erode an adversary's political will rather than produce decisive military effects.

Cyber capabilities should therefore not be understood as an independent instrument. They form part of a broader coercive toolkit that also includes ballistic missiles, drones, proxy militias, intelligence operations, hostage diplomacy, sanctions evasion, maritime pressure, information operations, and influence activity.

By integrating cyber capabilities into this wider framework, Tehran can maintain continuous pressure on its adversaries. Cyber operations allow Iran to retaliate against sanctions, respond to military strikes, collect intelligence, probe critical infrastructure, intimidate individuals, and signal displeasure while attempting to remain below the threshold of open conventional war.

This persistent, low-level confrontation enables Iran to preserve strategic relevance even when its conventional military capabilities, economic resources, or regional proxy networks are under significant pressure.

1.3 Strategic Objectives

Iran's cyber program is not a single-purpose capability. It is a portfolio of offensive, intelligence, disruptive, defensive, and influence capabilities that serve several mutually reinforcing strategic objectives.

Regime Survival and Deterrence

Cyber operations provide Iran with a comparatively low-cost and deniable means of imposing costs on adversaries while managing the risk of conventional retaliation. This logic is central to Tehran's broader defense doctrine, which relies on asymmetric and calibrated capabilities to compensate for its conventional military disadvantages relative to the United States, Israel, and several Gulf states.

Cyber activity can demonstrate reach, create uncertainty, and signal that military or economic pressure against Iran may produce consequences beyond the immediate area of conflict.

Intelligence Collection

A substantial proportion of Iranian cyber activity focuses on obtaining sustained access to sensitive communications, credentials, intellectual property, government information, technical data, and strategic networks. This activity supports the intelligence requirements of the IRGC, MOIS, military institutions, foreign-policy bodies, defense-industrial organizations, and the wider Iranian security establishment. Priority targets include government institutions, defense organizations, telecommunications providers, energy companies, technology firms, universities, political organizations, media outlets, dissidents, and individuals close to national decision-making.

Retaliation and Escalation Management

Cyber operations provide Iran with a flexible mechanism for responding to military strikes, sanctions, assassinations, diplomatic pressure, and other perceived provocations without necessarily committing to a proportional kinetic response. They can therefore serve both as instruments of retaliation and as tools for signaling resolve while attempting to control escalation. Cyber activity can be adjusted in intensity, visibility, target selection, and technical impact. This allows Tehran to impose costs while maintaining ambiguity regarding its intentions and level of direct involvement.

Suppression of Dissent

Iranian cyber capabilities are routinely directed against dissidents, journalists, activists, opposition organizations, civil-society groups, and diaspora communities. These operations extend the regime's domestic security and counterintelligence activities beyond Iran's territorial borders. They may include credential theft, account compromise, device surveillance, impersonation, doxing, network mapping, intimidation, and the identification of individuals who maintain relationships with foreign governments, media organizations, or opposition networks.

Psychological and Information Operations

Iranian actors increasingly combine technical compromise with influence activity. This can include hack-and-leak operations, impersonation, fabricated personas, coordinated amplification, SMS campaigns, manipulated media, website defacements, data exposure, and exaggerated or fabricated claims of operational success.

The objective is often not limited to technical damage. Iranian campaigns may seek to create fear, undermine trust in institutions, amplify political divisions, intimidate civilians, and reinforce the perception that Iran can penetrate the societies and organizations of its adversaries (Figure 1).

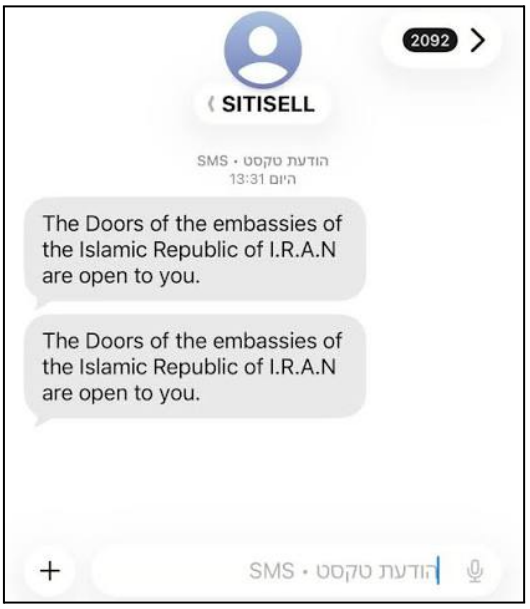


Figure 1 - An SMS sent to Israeli citizens as part of a psychological warfare campaign

1.4 Hybrid Conflict, Decentralization, and Operational Resilience

During the escalation that began in late February 2026, U.S. and Israeli strikes reportedly targeted elements of Iran's nuclear, missile, intelligence, cyber, electronic-warfare, military, and leadership infrastructure. Available reporting also indicates that some personnel associated with IRGC- and MOIS-linked cyber structures were killed or incapacitated.

The precise chronology, organizational consequences, and operational effects remain incompletely documented in authoritative open sources. Iran also experienced severe domestic connectivity disruption during this period. Some measurements indicated that national internet connectivity fell to a small fraction of normal levels, although the duration, geographic consistency, and technical causes of the disruption varied.

Such conditions would be expected to hinder operators dependent on infrastructure, personnel, or command channels located inside Iran. Open-source reporting suggested an initial reduction in visible state-linked activity originating from Iran. Proxy-associated, hacktivist, and ideologically aligned activity nevertheless continued or intensified. This pattern is consistent with several possible explanations, including pre-conflict preparation, delegated authority, standing target lists, independently motivated actors, external infrastructure, pre-positioned access, or contingency communications.

The available evidence does not establish that all observed activity was centrally directed in real time. Dozens of pro-Iranian collectives reportedly conducted reconnaissance, distributed denial-of-service attacks, website defacements, data-leak claims, and propaganda activity shortly after the escalation began. The rapid tempo of this activity is consistent with pre-existing preparation or delegated authority. However, it may also reflect independent ideological mobilization and opportunistic attempts by low-sophistication actors to exploit a major geopolitical crisis.

Within approximately 24 hours, some pro-Iranian channels began aggregating claims under a coordination label called the Electronic Operations Room. Its observable public role appeared closer to propaganda coordination, claim aggregation, amplification, and informal deconfliction than to a proven operational command structure. Reporting that some Iranian operators used satellite connectivity may indicate contingency planning, but, by itself, does not demonstrate a centrally organized continuity mechanism. Several weeks into the conflict, a major U.S. medical-technology company disclosed a cyber incident that prompted the precautionary isolation of parts of its global network.

Some public reports attributed the activity to an actor associated with Iran's Ministry of Intelligence and Security. However, the full scope of the compromise, the timing of initial access, and the precise chain of command remain unclear in open sources. The incident illustrates a broader analytical point: access established before a geopolitical crisis may survive leadership losses, infrastructure disruption, and changes in command. Previously deployed tooling, compromised credentials, external hosting, contractor-operated infrastructure, and long-term persistence can remain usable even when the personnel who originally authorized or supervised an operation are no longer available.

For analytical purposes, Iran's cyber ecosystem can be divided into three broad operational layers. The first consists of core state institutions, particularly IRGC- and MOIS-linked structures. These actors are associated with long-term espionage, strategic access, surveillance, counterintelligence, and higher-value operations. Leadership losses may degrade coordination, but they do not automatically remove access already established inside target environments.

The second consists of contractors, front companies, semi-official operators, and personas that may function as deniable extensions of state capability. These actors can provide technical services, operational infrastructure, access development, malware deployment, information operations, public claims, and attribution cover. The third consists of independent, opportunistic, ideologically aligned, or loosely affiliated hacktivists. Their activity is generally higher in volume and lower in sophistication. Their strategic value may lie less in direct operational impact than in generating noise, consuming defensive resources, amplifying propaganda, and obscuring more consequential activity.

This layered structure is broadly consistent with the logic of Iran's wider mosaic-defense concept, in which dispersed capabilities, delegated responsibility, redundancy, and local initiative are intended to preserve continuity when centralized structures are disrupted. However, the term should be used carefully. Not every independent or pro-Iranian actor should be assumed to operate under direct state control. The principal assessment is that disruption of Iran's cyber leadership should not be interpreted as evidence that the wider ecosystem has ceased to function.

Reduced visible activity may reflect genuine degradation, but it may also result from connectivity constraints, deliberate restraint, operational-security measures, internal reorganization, or efforts to preserve established access. Organizations should therefore assume that previously compromised identities, persistent access, contractor-operated infrastructure, delegated operators, and proxy networks may remain available during and after periods of military escalation.

Strategic Implications

Leadership decapitation and infrastructure strikes may reduce short-term coordination. However, such disruption should not automatically be interpreted as producing a proportional reduction in cyber risk. Organizations should assume that pre-positioned access, compromised credentials, delegated operators, external infrastructure, and proxy capabilities may remain operational. Periods immediately following geopolitical escalation create an important opportunity for threat hunting, as disrupted operators may expose infrastructure, change procedures, or activate previously dormant access. Governments and critical infrastructure operators should prioritize identity security, network segmentation, detection of long-term persistence, third-party risk management, operational technology exposure, and continuous monitoring.

1.5 Evolution of Iranian Cyber Strategy

Iran's cyber program did not emerge from a single, coherent doctrine. It developed incrementally in response to strategic shocks that exposed both Iran's vulnerability to cyber operations and the value of cyber capabilities as instruments of intelligence collection, retaliation, coercion, influence, and domestic control.

The most consequential early turning point was the Stuxnet operation, disclosed in 2010. The sabotage of centrifuges at the Natanz nuclear facility demonstrated that cyber operations could cause physical damage to strategic infrastructure. For Iranian decision-makers, the incident reinforced two conclusions: Iran needed greater protection and control over its domestic digital environment, and it required the ability to impose cyber costs on external adversaries. Because cyber operations are difficult to attribute and can be calibrated more easily than overt military action, they offered Tehran an attractive means of responding to external pressure while limiting the risk of immediate escalation.

Over the following years, Iran moved beyond a predominantly defensive and censorship-oriented posture and began developing more substantial offensive, disruptive, and intelligence-collection capabilities. The 2012 Shamoon attack against Saudi Aramco, which affected approximately 30,000 computers, demonstrated Iran's growing willingness and ability to conduct large-scale, destructive operations against regional adversaries. Between approximately 2012 and 2020, Iranian actors expanded both disruptive capabilities and long-term espionage infrastructure. Distributed denial-of-service campaigns against U.S. financial institutions, the intrusion into a dam in Rye, New York, and successive waves of destructive malware illustrated Tehran's willingness to target financial services, industrial systems, and critical infrastructure.

During the same period, Iranian actors developed more persistent cyber-espionage capabilities. Groups commonly tracked as APT33, APT34, APT35, and related clusters targeted the energy, aviation, defense, telecommunications, government, academic, and policy sectors. The 2018 U.S. indictment of individuals associated with the Mabna Institute provided important insight into Iran's contractor-based operational model. It showed how nominally private or academically oriented organizations could conduct state-directed collection while also monetizing stolen information or access through domestic commercial channels.

A further evolution occurred between approximately 2020 and 2023, as Iranian operations increasingly blurred the distinction between covert espionage and overt disruption. Tehran-linked actors adopted hacktivist branding, leak personas, ransomware-like behavior, and ideologically framed public messaging. Personas such as CyberAv3ngers, Moses Staff, Black Shadow, and others presented themselves as independent or politically motivated groups, although subsequent sanctions, technical analysis, and government assessments linked several of them to Iranian state institutions or state-associated operators.

This model provided Tehran with significant operational flexibility. An intrusion could begin as intelligence collection, evolve into data theft or destructive activity, and later be publicly presented as an independent hacktivist operation. The technical operation and the public narrative could therefore serve different but complementary objectives: intelligence collection, coercive signaling, psychological pressure, reputational damage, and plausible deniability.

The conflict that followed October 2023 accelerated this evolution. The war in Gaza triggered a broad mobilization of pro-Iranian and anti-Israel cyber personas. Groups such as Handala, Karma Group, and Mobir Team emerged or increased their visibility through data-leak claims, disruptive activity, doxing, propaganda, and psychological messaging. Much of this activity was low in technical sophistication, exaggerated, recycled, or difficult to verify. Nevertheless, it demonstrated the ability of Iran and aligned actors to generate a high volume of cyber-related claims and influence activity during an active military conflict.

The June 2025 conflict further illustrated the increasing synchronization of cyber operations with kinetic escalation. Operational tempo, target selection, and propaganda narratives appeared increasingly responsive to battlefield developments, political events, and Iranian strategic messaging. This did not necessarily indicate the centralized direction of every operation. Rather, it reflected a wider ecosystem in which state-linked actors, contractors, proxies, hacktivists, and independently motivated groups could contribute to a common strategic effect.

The strikes against Iranian leadership and cyber-related infrastructure in 2026 may represent another important inflection point. Open-source reporting suggests that elements of Iran's centralized cyber leadership, coordination mechanisms, and supporting infrastructure were degraded. At the same time, contractor, proxy, and hacktivist activity continued, indicating that parts of the wider ecosystem remained operational despite disruption at the state-command level.

These developments are consistent with a more decentralized and resilience-oriented operational model. Iran's cyber capacity is increasingly distributed across state institutions, semi-autonomous contractors, front companies, proxy-linked actors, hacktivist personas, criminal intermediaries, and externally hosted infrastructure. This structure reduces dependence on any single command center or operational team and allows previously established access, delegated operators, and external infrastructure to remain useful during periods of leadership loss or connectivity disruption.

The concept of a cyber "mosaic defense" provides a useful analytical framework for understanding this model, provided it is not interpreted as proof that every pro-Iranian actor is centrally controlled. The system's resilience lies precisely in its mixture of direct state tasking, delegated authority, ideological alignment, opportunistic participation, and varying degrees of operational autonomy.

The long-term trajectory is therefore one of adaptation rather than retreat. As Iran's conventional freedom of action becomes more constrained, cyber capabilities are likely to assume greater importance in intelligence collection, retaliation, coercive signaling, influence activity, sanctions evasion, and support to proxy networks.

The operational center of gravity may continue to shift away from direct execution by identifiable state institutions and toward strategic tasking, financing, access management, capability development, and coordination across a broader contractor and proxy ecosystem.

Iran's evolving cyber strategy should therefore not be assessed solely through the activity of individual APT groups. Its principal strength lies in the ability of a distributed ecosystem to preserve operational continuity, generate ambiguity, and support Iranian strategic objectives under sustained military, economic, political, and technological pressure.

2. Understanding Iran's Cyber Power

2.1 Strategic Leadership and Decision-Making

Formal authority over Iran's cyberspace policy rests with the Supreme Council of Cyberspace (SCC), established by Khamenei's decree in March 2012 and consolidated in 2015, when several overlapping bodies were folded into it. On paper, the SCC is chaired by the president and includes the heads of the judiciary, parliament, and relevant ministries; in practice, roughly a third of its members are Khamenei's direct appointees, its decrees carry the force of law and are explicitly shielded from administrative and judicial review, and its executive arm, the National Center of Cyberspace, answers up the same chain.

This institutional structure is designed to keep cyberspace policy and censorship under the authority of the Supreme Leader’s office, regardless of who holds the presidency. It may also provide strategic oversight relevant to offensive cyber policy, although the precise relationship between the SCC and operational cyber tasking remains opaque. Personnel changes at the top (the 2023 appointment of the hardline Mohammad Amin Aghamiri as SCC secretary, tied to the Basij, is illustrative) tend to track the broader security establishment's posture rather than any independent technology policy logic.

The February 2026 strikes reportedly caused significant disruption within Iran’s intelligence, security, and cyber-related leadership structures. Open-source reporting indicated that several senior Iranian intelligence and security officials were killed, including Yahya Hosseini Panjaki, also known as Yahya Hamidi. Public reporting primarily describes him as a senior MOIS official associated with internal security, Israel-related intelligence, and external operations. Claims linking him directly to specific cyber command functions, operational cyber units, or hacktivist personas remain insufficiently corroborated.

Because available sources differ regarding the precise scope of his responsibilities and organizational position, this report treats those details as unconfirmed pending authoritative corroboration. In addition, open-source reporting indicated that facilities described as the IRGC’s cyber warfare headquarters and elements of its intelligence directorate in eastern Tehran were targeted. These strikes may have disrupted elements of the centralized command, coordination, and communications supporting Iranian cyber activity and may have required significant organizational reconstitution. The operational consequence is not that Iranian cyber capability disappeared; indeed, visible proxy- and contractor-associated activity continued or re-emerged within hours. Rather, the tempo and coherence of some centrally tasked operations appear to have degraded while the relative autonomy of hacktivist fronts, criminal-linked actors, and university-adjacent contractors has grown by default.

Any authority that reconstitutes the command layer may inherit a program that has become more distributed and less centrally auditable than before.

2.2 The IRGC and MOIS Cyber Architecture

Iran's security, intelligence, and cyber architecture (Figure 2) is not a single centralized system, but a layered ecosystem shaped by institutional rivalry, ideological control, military doctrine, and regime-protection priorities. At its core are the Islamic Revolutionary Guard Corps, the Ministry of Intelligence, and the regular armed forces, each maintaining distinct but sometimes overlapping cyber, intelligence, counterintelligence, and influence capabilities.

These bodies operate through formal military and intelligence structures, semi-official contractors, academic and technical networks, proxy organizations, and deniable cyber personas. Understanding this architecture is essential for assessing Iranian cyber operations, because campaigns often reflect not only technical objectives but also Iran's broader security-state priorities, competition, and coordination patterns.

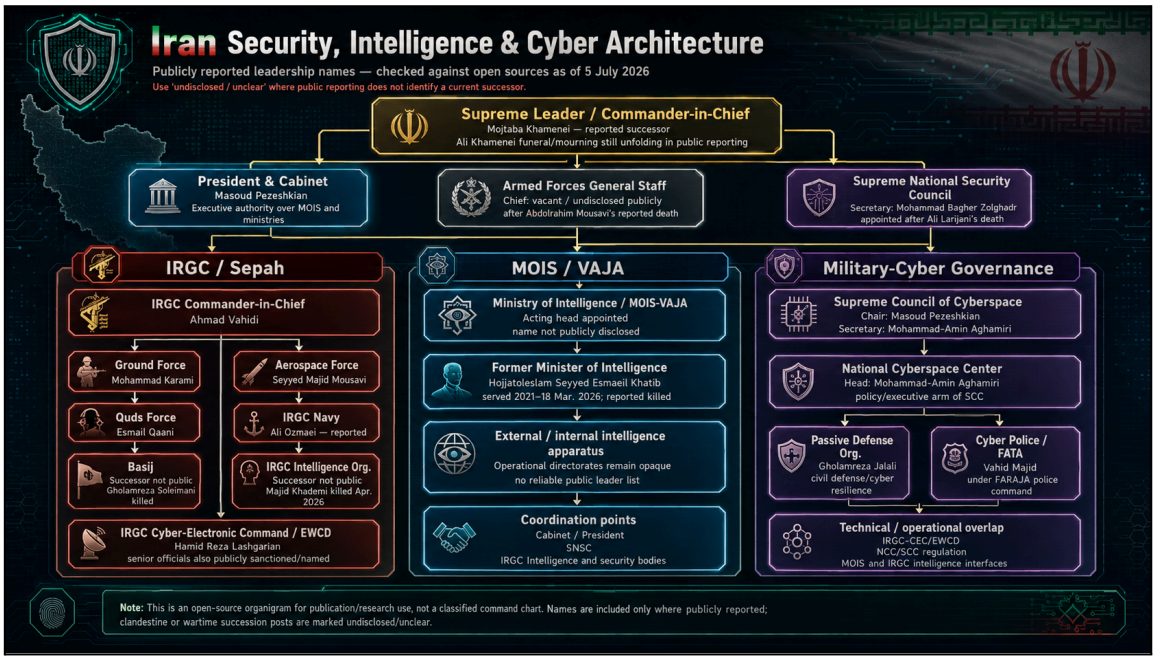


Figure 2 - Iran's security, intelligence, and cyber architecture

The Islamic Revolutionary Guard Corps (IRGC) cyber architecture is built around three main pillars**.** Its Intelligence Organization has been associated with activity tracked under labels including APT35, Charming Kitten, Mint Sandstorm, and APT42. These overlapping industry designations generally describe clusters focused on social engineering, credential theft, surveillance, and intelligence collection against diplomats, journalists, dissidents, academics, activists, and nongovernmental organizations. The IRGC Cyber-Electronic Command (IRGC-CEC) represents the more operationally and militarily oriented component of this architecture and has been directly tied, through 2024 Treasury sanctions, to the CyberAv3ngers operations against U.S. and allied industrial control systems, as well as to front entities such as Mahak Rayan Afraz.

A third pillar, the Basij Cyber Council, functions as a volunteer paramilitary layer that can supply lower-skilled personnel for website defacements, distributed denial-of-service attacks, and information operations under varying degrees of IRGC supervision. Its value lies primarily in operational volume, ideological mobilization, and deniability rather than in consistently sophisticated tradecraft.

The Ministry of Intelligence and Security operates a parallel but organizationally distinct set of capabilities that generally emphasizes sustained intelligence collection, surveillance, and covert access over overt ideological branding. APT34 (OilRig), one of the longest-running Iranian intrusion sets, favors patient webshell deployment and credential harvesting against government, financial, and energy targets across the Gulf and beyond; MuddyWater conducts similarly long-horizon espionage, increasingly through living-off-the-land techniques and custom backdoors such as the recently documented Dindoor; and APT39, operating historically through the Rana Intelligence Computing front, has focused on domestic surveillance of dissidents alongside external targeting, to the point that some of its personnel have been directly linked to physical plots against Iranian dissidents abroad. Available government and threat intelligence reports have linked the Void Manticore cluster and the Handala persona to MOIS-associated activity. However, the precise organizational relationship, command structure, and degree of direct operational control remain unclear. This attribution has also evolved over time, illustrating the continuing difficulty of distinguishing between IRGC-, MOIS-, contractor-, and persona-based activity within the Iranian cyber ecosystem.

In practice, the line between these two architectures is considerably less distinct than official organizational charts suggest. Multiple documented operations reveal shared infrastructure, overlapping tooling, and borrowed tactics, techniques, and procedures (TTPs) across nominally separate IRGC- and MOIS-attributed clusters. This blurring is likely driven by overlapping contractor pools, personnel mobility, shared service providers, or common technical resources. While direct inter-agency coordination may also account for some of these similarities, the exact extent of this collaboration remains unclear.

This structural ambiguity provides Tehran with significant operational utility. It complicates foreign attribution, allows each service to plausibly deflect blame, and ensures systemic resilience. Consequently, the reported degradation of individual nodes within the IRGC command infrastructure during the February 2026 escalation would not necessarily eliminate the underlying technical capability. Because parts of this apparatus are distributed across external contractors, some capabilities may potentially be re-tasked by institutions that retain functioning command authorities, financial resources, and access to the relevant personnel or infrastructure.

2.3 Universities, Contractors, and the Innovation Ecosystem

Iran's cyber capability is sustained not only by uniformed or government personnel, but also by a competitive marketplace of ostensibly private contractors that develop capabilities, provide infrastructure, recruit personnel, and execute state-directed tasks. A Recorded Future assessment published in 2019 estimated that as many as 50 organizations competed for IRGC-linked cyber contracts. Although the current number is unknown, the estimate illustrates the breadth of the contractor environment. The Mabna Institute, whose 2018 indictment exposed this model in considerable detail, provides one of the clearest examples. At the direction of the IRGC, its operators reportedly compromised approximately 8,000 email accounts belonging to professors at more than 300 universities worldwide. Rana Intelligence Computing (linked to APT39 and later sanctioned in full, down to forty-five individual employees), Emennet Pasargad and its successor entity Aria Sepehr Ayandehsazan (IRGC-linked, focused on election interference and hack-and-leak work), and Ravin Academy, a MOIS-founded training company that recruits and develops offensive operators, round out a picture of an ecosystem that looks, administratively, much like any other outsourced government contracting environment.

This contractor layer is fed directly by the university system, and deliberately so. Iranian technical universities function as both a talent pipeline and a recruitment ground. The founders of the Mabna network described their company's original purpose as helping Iranian universities and research institutes access scientific resources otherwise blocked by sanctions, a mission that quickly shifted into commercial and state-directed hacking. Historic hacking forums such as Ashiyane, which trained a generation of Iranian hackers from the mid-2000s onward, functioned as an informal finishing school that fed capability into both criminal and state-aligned work long before any formal contracting relationship existed, and that same informal-to-formal pipeline persists today. Iran has treated this as a budget priority rather than an afterthought: cyber spending was reported at around one billion dollars annually by the mid-2010s, while subsequent investments indicate that cyber capability has remained a strategic priority, with a stated ambition to significantly expand the digital economy's share of GDP by the middle of this decade.

Isolation from global technology markets, rather than weakening this ecosystem, has, if anything, reinforced it. Sanctions that cut Iranian firms off from Western cloud, software, and hardware markets have pushed talent and investment inward, toward a domestic contracting and training ecosystem that is harder for outside pressure to reach than a state-run military unit would be.

2.4 Proxy, Criminal, and Hacktivist Networks

Iran's use of proxy and hacktivist networks in cyberspace is best understood as the digital extension of a strategic doctrine it has practiced for decades on the ground: build layers of deniable actors between the regime and the attack so that retaliation, if it comes, has no clean target. What analysts have come to call Iran's "mosaic defense" doctrine in cyberspace, deliberate fragmentation across dozens of semi-independent fronts rather than concentration in a small number of easily-targeted units, may reflect a combination of deliberate resilience, institutional fragmentation, contractor dependence, and operational evolution.

The CyberAv3ngers case remains one of the clearest examples: a group that spent months building credibility as an ideologically driven, Gaza-focused hacktivist outfit was later publicly linked by U.S. Treasury sanctions to the IRGC Cyber-Electronic Command, with access to funding, infrastructure, and technical capabilities beyond those typically associated with independent hacktivists. The same pattern may be observed in reporting on Handala. Government and threat-intelligence sources have linked the persona to Void Manticore and MOIS-associated activity, although the precise organizational relationship and degree of direct operational control remain unclear.

The scale of this ecosystem expands sharply whenever conflict escalates, and the timeline since October 2023 shows the mechanism clearly: the Gaza war produced a first wave of new personas (**Handala Hack Team, Karma Group, Mobir Team** among them); the June 2025 Twelve-Day War demonstrated that dozens of these groups could synchronize disruptive tempo with an active military campaign. The February 2026 strikes reportedly triggered an even broader mobilization, with more than 60 pro-Iranian hacktivist groups claiming activity within hours. Some threat-intelligence firms described elements of this mobilization as part of an “Islamic Resilience Cyber Axis,” a loosely defined coalition reportedly including pro-Hamas and other ideologically aligned actors operating beyond Iran’s borders. (Figures 3, 4 and 5). Much of this claimed activity is unverified or exaggerated, which is itself part of the doctrine: volume and noise impose a defensive burden on targets regardless of how much of it is real.

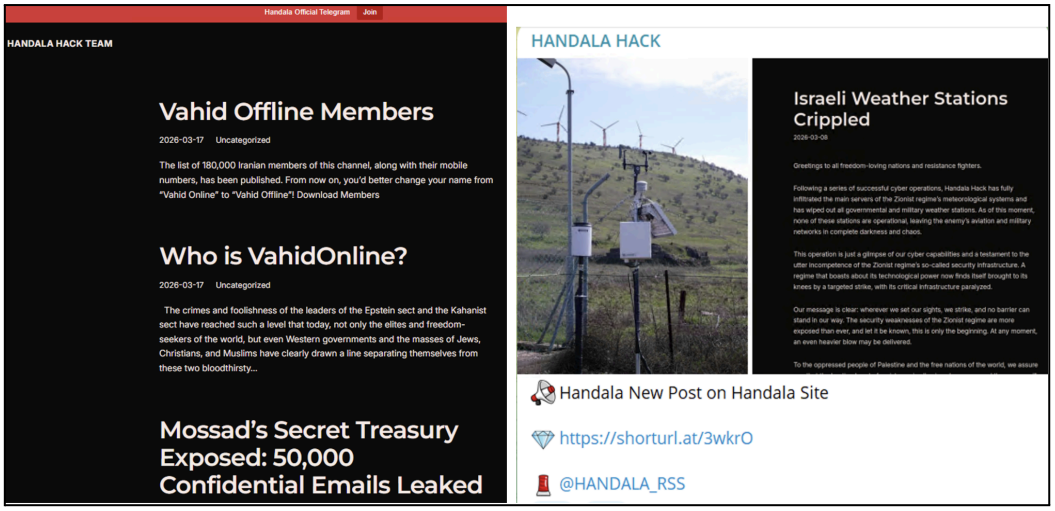


Figure 3 - Claims of cyber operations against Israeli targets published by the Handala Hack Team on its website and Telegram channel.



Figure 4 - Telegram message from the Cyber Islamic Resistance group claiming a series of cyberattacks against what it describes as the "Zionist regime"



Figure 5: An Iran-aligned threat actor using the name APT IRAN claims to have attempted to target Jordanian critical infrastructure.

Additionally, pro-Russian hacktivist groups, including NoName057(16) and Server Killer, have claimed denial-of-service attacks and data compromises against Western and Israeli targets in support of Iran (Figure 6).



Figure 6 - Telegram post from the pro-Russian group NoName057(16) claiming cyber operations against Israeli organizations.

Threat actors such as Pioneer Kitten have been reported to combine state-aligned access operations with financially motivated activity, including access brokering and ransomware-related collaboration. The extent to which individual operations were directly tasked, independently monetized, or conducted with state authorization may vary by campaign. Regionally, this proxy logic may also extend to cyber capabilities associated with Hezbollah, Hamas, and Houthi-aligned actors. Public reporting has described varying forms of Iranian training, technical assistance, resourcing, infrastructure sharing, and strategic support to regional partners. The nature and degree of direct IRGC involvement differ across organizations and operations and should not be assumed to be uniform. As Iran's physical supply lines to regional partners have come under increased pressure, cyber-enabled support may become comparatively more important because training, tooling, infrastructure sharing, and remote technical assistance can be delivered without the physical movement of equipment or personnel across contested borders. The net effect is a threat surface that is resilient almost by design: degrading the state core may slow the system, but it does not eliminate its wider operational capacity because so much of the actual operational tempo is already distributed across contractor, proxy, and semi-autonomous operational layers.

2.5 International Military and Cyber Partnerships and Support

2.5.1 Military Cooperation

Iran - Russia

Russia-Iran military relations have become among the most consequential in practice, primarily because of their direct relevance to ongoing conflict dynamics. The core of the relationship lies in military-technical cooperation, particularly in unmanned aerial systems. U.S. and allied assessments indicate that Iran has supplied Russia with large numbers of one-way attack UAVs, in the style of HESA Shahed 136 Gen 2 (Figure 7), used extensively in Ukraine. These systems have been integrated into Russia's strike campaign against critical infrastructure. Beyond transfers of finished systems, reporting also suggests the development of local production capacity in Russia with Iranian support, indicating a deeper level of industrial and technological interaction.

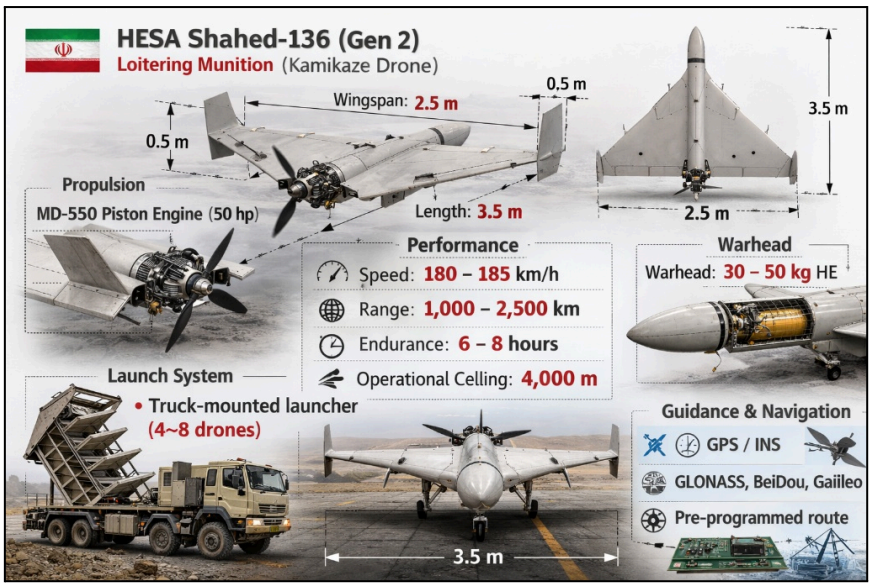


Figure 7 - Overview and reported specifications of the Iranian Shahed-136 family of one-way attack UAVs.

In 2016, Russia completed the delivery of S-300PMU-2 "Favorit" surface-to-air missile systems to Iran (Figure 8). Additionally, according to the US Department of Defense, Iran transferred short-range ballistic missiles to Russia in 2024. While several governments publicly confirmed these transfers, some operational details, including deployment patterns and associated systems, remained less clearly established in initial reporting.



Figure 8 - Overview and specifications of Russian S-300PMU-2 "Favorit" surface-to-air missile

What distinguishes this relationship is the combination of battlefield utility and emerging industrial cooperation. Iran is not only a supplier of systems, but also a contributor to Russia's ability to sustain and scale production under sanctions constraints. At the same time, the relationship should not be overstated. As of early 2026, there is no verified open-source evidence that Russia has entered Middle Eastern conflicts militarily on Iran's behalf. The partnership remains highly significant but is primarily defined by wartime support to Russia rather than a broader alliance structure.

Iran - China

China-Iran military relations are real but remain deliberately limited and carefully calibrated. The most visible dimension is maritime cooperation, including joint naval exercises conducted with Russia in the Gulf of Oman. These activities serve a signaling function and reflect shared interests in regional stability and maritime security, particularly in areas linked to energy flows. Beyond exercises, the relationship includes documented concerns regarding procurement networks linked to Iran's missile and UAV programs. Sanctions designations by U.S. authorities have identified entities based in China connected to the supply of dual-use materials and components to Iranian defense-industrial actors. There have also been reports that Iran is seeking to acquire advanced Chinese anti-ship missile systems. As of early 2026, these should be treated as prospective or reported negotiations rather than confirmed transfers. Overall, China appears to approach military cooperation with Iran cautiously. While Beijing values Iran strategically, particularly for energy security and regional influence, it has avoided deep military integration that could increase the risk of direct confrontation with the United States or its partners. The relationship is therefore best understood as selective and pragmatic rather than alliance-driven (Figure 9).



Figure 9 - Iran- China military relations

Iran - North Korea

Iran-North Korea military relations are the least visible but remain important, given their focus on missile and proliferation-related cooperation. The most solid publicly documented evidence comes from United Nations reporting indicating that the two countries have cooperated on long-range missile development, including the transfer of components and the provision of technical support. This relationship is not characterized by joint exercises, formal treaties, or visible operational coordination. Instead, it is best understood as a long-term, low-visibility exchange centered on missile technology and expertise. Both countries are heavily sanctioned and share incentives to collaborate in ways that bypass international controls (Figure 10).

Recent open-source reports provide fewer concrete details about ongoing transfers compared to earlier periods, and there is no strong public evidence of expanded military cooperation in the 2024-2026 timeframe. Political alignment and rhetorical support exist, including North Korean backing of Iran in the current Middle East crisis, but this does not constitute proof of active military assistance. As a result, Iran-North Korea should be treated as a proliferation-focused relationship with potentially significant long-term implications, but limited visible operational activity.



Figure 10 - Iran- North Korea military relations

2.5.2 Cyber Cooperation

Russia

Iran's broader relationship with Russia creates opportunities for technical exchange, operational learning, and exposure to Russian surveillance, electronic-warfare, and intelligence capabilities. Publicly available evidence of systematic, operational-level cyber cooperation remains limited, however, and similarities in tactics or strategic interests should not automatically be interpreted as proof of direct technology transfer or joint cyber operations.

China

With China, cooperation is closely tied to infrastructure and technology transfer. Chinese telecommunications firms have played an important role in the development of Iran's communications and digital infrastructure. Some reporting has linked Chinese-origin technologies to capabilities relevant to network management, monitoring, and internet filtering. The degree to which these commercial relationships translate into direct state-to-state cyber cooperation remains unclear. This has strengthened Iran's ability to control and secure its domestic information space.

North Korea

Iran's interaction with North Korea is most clearly observed in overlapping cyber tactics and operations, particularly in financially motivated cyber activity. Both countries have conducted cyber-enabled financial operations targeting cryptocurrency platforms and financial institutions. Similarities in operational objectives and tradecraft may reflect parallel adaptation to sanctions pressure, shared learning, limited technical exchange, or independent convergence. Public evidence is insufficient to determine the extent of direct operational cooperation.

2.6 Financing, Sanctions Evasion, and Crypto-Enabled Infrastructure

Iran's restricted access to SWIFT, dollar-clearing mechanisms, and other components of the international financial system has increased the strategic relevance of cryptocurrency for sanctions evasion, cross-border payments, capital preservation, cybercrime, and the financing of state-linked or proxy activity. Industry reporting indicates that Iran-associated cryptocurrency activity reached several billion dollars in 2025, although estimates vary according to address attribution, clustering methodology, and the categories of activity measured.

Some blockchain analysis reported that addresses attributed to IRGC-linked entities accounted for a significant share of identified Iran-associated activity during parts of 2025 (Figure 11). These findings depend on the address-attribution and clustering methodologies used and should not be interpreted as a verified measure of the entire Iranian cryptocurrency economy. Nobitex, widely described as Iran's largest cryptocurrency exchange, has processed a significant proportion of the country's reported digital-asset activity.

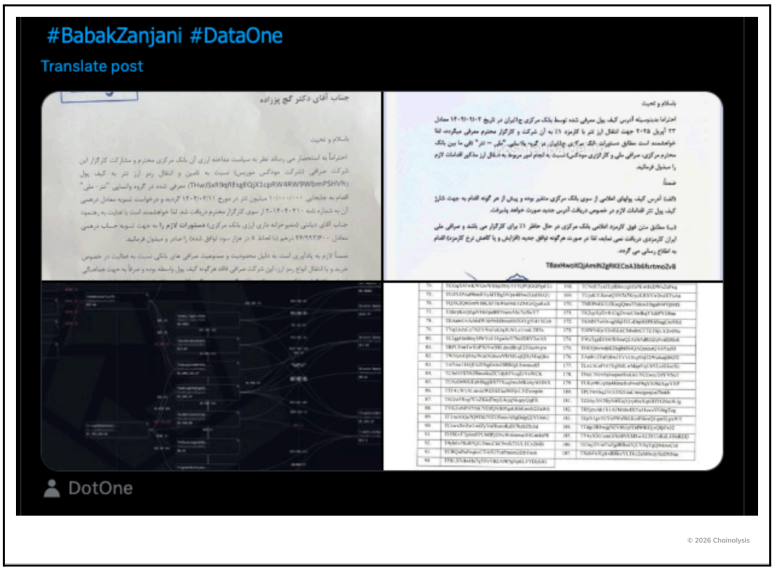


Figure 11- Documents presented as Central Bank of Iran records and circulated through social-media accounts, allegedly identifying cryptocurrency addresses associated with Iranian state entities. The authenticity of the documents and the attribution of the addresses have not been independently verified. (Source: Chainalysis).

In June 2026, the U.S. Department of the Treasury's Office of Foreign Assets Control designated four major Iranian digital-asset exchanges Nobitex, Wallex, Bitpin, and Ramzinex as part of a broader effort to disrupt financial channels associated with sanctioned Iranian entities. The action represented a deliberate expansion of financial pressure against Iran's domestic digital-asset ecosystem. Available reporting indicates that some of the financial and procurement mechanisms supporting Iranian cyber operations intersect with this broader sanctions-evasion and gray-market architecture, although the extent and organizational consistency of these relationships remain difficult to establish.

Material published in December 2025 and presented as leaked internal records associated with Iranian cyber operations appeared to contain information concerning domain registrations, European virtual private server hosting, cryptocurrency payments, administrative records, and possible operational links among multiple personas. Some researchers assessed that the records reflected shared procurement and administrative processes connected to APT35- and Moses Staff-related activity.

However, the authenticity, completeness, provenance, and attribution of the material have not been independently established. It should therefore be treated as supporting or circumstantial evidence rather than definitive proof of a unified operational command structure or direct state control over every activity documented in the records.

Cryptocurrency infrastructure used for ransomware, cyber-enabled extortion, infrastructure procurement, and hack-and-leak activity may intersect with broader financial networks serving sanctioned state entities, intermediaries, and regional proxies. Western enforcement actions appear to have disrupted particular channels and may have prompted tactical adaptation, but the available evidence does not yet demonstrate comprehensive or lasting structural disruption.

In 2026, actions by the U.S. Department of the Treasury's Office of Foreign Assets Control, together with measures taken by U.S. authorities and private stablecoin issuers, resulted in the designation of cryptocurrency addresses linked to Iranian entities and the freezing or restriction of access to significant digital-asset holdings. These actions should be assessed on a case-by-case basis. Their strategic impact depends on the specific legal authority used, the blockchain and addresses involved, the role of intermediaries, the method of asset restriction, and the evidence supporting beneficial ownership. OFAC designations, asset blocking, issuer-administered token freezes, and judicial seizures should therefore be distinguished from one another and should not be aggregated or described as a single Treasury seizure without clear supporting documentation.

Iran is likely to continue seeking access to international cryptocurrency liquidity through domestic exchanges, offshore intermediaries, informal brokers, decentralized financial services, and relationships with other sanctioned networks. In some circumstances, the financial and operational costs of using digital assets may remain lower than those associated with transferring equivalent funds through heavily restricted conventional banking channels. Enforcement may therefore increase transaction costs, expose intermediaries, and disrupt specific financial pathways without necessarily eliminating crypto-enabled financing altogether.

Intelligence Assessment

- Iran's cyber architecture should be understood as an ecosystem rather than a centralized command structure.
- The contractor model significantly increases resilience by distributing expertise, infrastructure, and operational responsibility across multiple organizations.
- Consequently, targeting individual actors or front companies is unlikely to produce lasting strategic effects unless accompanied by disruption of recruitment pipelines, financial networks, and technological infrastructure.

3. The Iranian Operational Model

3.1 How Iran Builds Cyber Operations

The Iranian regime builds cyber operations through a hybrid ecosystem rather than through a single, cleanly centralized cyber command. This is one of the most important features of the Iranian model: Tehran combines state organs, especially IRGC- and MOIS-linked structures, with semi-deniable contractors, patriotic hackers, criminal-adjacent operators, proxy-aligned personas, and information-operation channels. The result is an operational architecture capable of conducting espionage, harassment, disruption, coercive messaging, and psychological operations while preserving plausible deniability. Unlike Russia, which often relies on highly capable military-intelligence cyber units, or China, which emphasizes industrial-scale strategic collection, Iran's model is more opportunistic, modular, and politically integrated. Access may be developed by one actor, weaponized by another, claimed by a persona, and amplified by state-aligned media or Telegram networks. Microsoft's reporting after October 7, 2023, showed this dynamic clearly:

Iranian activity against Israel initially appeared hasty and sometimes poorly coordinated, but quickly evolved into a broader campaign involving multiple Iranian groups, cyber personas, destructive claims, leaks, and influence activity designed to weaken Israeli morale and international support.

The actionable intelligence point is that Iran's cyber system should be mapped as an ecosystem of functions rather than only as named APT groups: access brokers, phishing teams, destructive operators, leak personas, media amplifiers, and proxy-aligned narratives are often part of the same strategic effect even when technical infrastructure differs.

3.2 Intelligence Collection and Target Development

Iranian target development is heavily human-centric: before Tehran compromises networks, it often studies people, relationships, travel patterns, professional affiliations, political positions, and personal vulnerabilities. This reflects the regime's intelligence culture, where cyber activity supports counterintelligence, regime protection, foreign-policy collection, proxy warfare, and surveillance of dissidents. APT42 is the clearest public example.

The cyber intelligence company Mandiant (By Google) assesses that APT42 operates on behalf of the IRGC Intelligence Organization and targets Western and Middle Eastern NGOs, media organizations, academia, legal services, activists, and individuals of strategic interest to Iran. Its operations rely on carefully crafted social engineering, impersonation, credential harvesting, and cloud account compromise rather than solely on malware deployment. Google TAG reported that APT42 targeted high-profile users in Israel and the United States, including government officials, diplomats, political campaigns, think tanks, NGOs, and academics.

This is strategically significant because Iran often develops targets through communities rather than through sectors alone: Iran experts, former officials, journalists, nuclear specialists, Israeli military-linked individuals, sanctions analysts, and diaspora activists can serve as gateways into broader intelligence problems. Actionable indicators include unsolicited journalist approaches, conference invitations, fake policy roundtables, suspicious encrypted-messaging outreach, credential-harvesting pages imitating cloud services, and attempts to bypass MFA through social pressure or repeated login prompts.

3.3 Operational Tradecraft

Iranian operational tradecraft is uneven but effective because it is adapted to Tehran's strategic needs. Some Iranian actors demonstrate relatively basic intrusion behavior: credential theft, exploitation of exposed services, web shells, abuse of legitimate remote-access tools, phishing, default-password exploitation, and opportunistic targeting of vulnerable public-facing infrastructure. Other actors demonstrate more advanced persistence and access management capabilities. Mandiant's reporting on UNC1860, assessed as likely affiliated with Iran's Ministry of Intelligence and Security, describes a persistent Iranian state-sponsored actor operating across Middle Eastern government and telecommunications networks, with passive backdoors and tooling that may support long-term access for multiple Iranian operations.

This distinction matters. Iran's cyber strategy does not require every actor to be technically elite; it requires sufficient persistent access, sufficient psychological effect, and sufficient ambiguity to support coercive statecraft. Iranian tradecraft often blends stealth and noise: quiet espionage may continue for months, but once a political trigger occurs, access can be exposed through leaks, wipers, public claims, or intimidation messages. The actionable analytic approach is therefore behavioral: look for infrastructure reuse, lure reuse, persona overlap, synchronized disclosure, and the transition from collection to exposure. When an Iranian-linked operation shifts from quiet access to public messaging, it often indicates that strategic signaling has become more valuable than continued intelligence collection.

3.4 Cyber Espionage Operations

Iranian cyber espionage is designed to answer regime-relevant questions: What are Israel, the United States, the Gulf states, and European governments planning? Who is working against the Iranian regime? Which sanctions, covert actions, military deployments, nuclear negotiations, or opposition networks threaten Tehran? The collection priorities are therefore political, military, ideological, and counterintelligence-driven.

APT42's focus on officials, journalists, activists, legal professionals, academics, and policy experts shows how Iran targets individuals who sit close to decision-making, wield influence, or operate within sensitive networks. Google and Mandiant have described APT42 as an Iranian state-sponsored actor linked to the IRGC Intelligence Organization, using advanced social engineering and credential theft against Western and Middle Eastern NGOs, media organizations, academia, legal services, activists, Israeli targets, and accounts connected to the U.S. presidential election.

This demonstrates a core Iranian method: rather than attacking networks directly, Tehran often targets the people around power advisers, researchers, campaign staff, journalists, dissidents, and policy specialists to access private communications, political intentions, and strategic assessments.

This pattern has been visible in several significant campaigns. Against Israel and Israeli-linked targets, APT42 has intensified phishing operations aimed at officials, former military personnel, diplomats, researchers, and civil society figures, often by impersonating journalists, policy experts, or trusted professional contacts. These operations are valuable because Israeli political, military, and security decision-making is often distributed across government, reservist networks, think tanks, media, academia, and private technology companies. By compromising personal email, cloud accounts, or messaging platforms, Iranian operators can collect intelligence on Israeli threat perceptions, internal debates, military escalation scenarios, and connections between state and non-state actors. In parallel, fake emergency-warning and "Red Alert"-style mobile operations targeting Israeli users illustrate how espionage can exploit crisis psychology (Figures 12 and 13).



Figure 12 - Fake Emergency RedAlert App (Source: CloudSek)

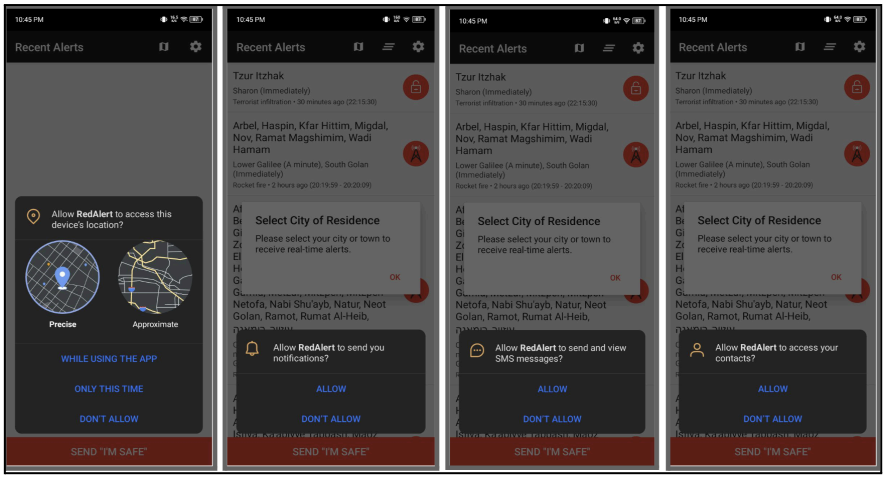


Figure 13 - Fake Emergency Red Alert App user interface (Source: CloudSek)

Trojanized alert applications and spoofed Home Front Command-style messages abuse civilian dependence on real-time missile-warning systems, turning fear, urgency, and public-safety trust into opportunities for device surveillance, contact harvesting, location tracking, and psychological pressure.

Against the United States, Iranian cyber-espionage campaigns have focused on political campaigns, government-linked individuals, critical infrastructure, defense, satellite communications, oil and gas, and policy communities. APT42's targeting of accounts associated with the U.S. presidential election reflects Tehran's interest in understanding, shaping, or preparing for future U.S. policy toward Iran. Separately, Microsoft reported that Peach Sandstorm, also tracked as APT33 or Refined Kitten, deployed the custom Tickler backdoor in 2024 against targets in the satellite, communications equipment, oil and gas, and federal and state government sectors in the United States and the United Arab Emirates. These campaigns show that Iranian espionage is not limited to political intelligence; it also seeks insight into military readiness, space and communications infrastructure, energy security, and the technological systems that support U.S. and allied power projection.

Across the wider Middle East, Iranian operators have repeatedly targeted telecommunications, government, defense, aerospace, energy, and diplomatic networks. UNC1860, assessed by Mandiant as a persistent Iranian state-sponsored actor likely linked to Iran's Ministry of Intelligence and Security, has maintained specialized tools and passive backdoors for access to high-priority Middle Eastern government and telecommunications environments. This type of access is strategically important because telecom networks can support surveillance, geolocation, lawful-intercept abuse, regional intelligence collection, and preparation for future disruptive operations.

OilRig/APT34 provides another example of Iran's regional espionage model: it has long targeted Middle Eastern organizations and has used supply-chain style access and custom malware downloaders against Israeli and regional victims. Together, these campaigns suggest that Iran's cyber-espionage architecture is built around three complementary layers: human intelligence through phishing and social engineering, strategic network access through telecom and government intrusions, and opportunistic exploitation of regional crises through fake applications, spoofed alerts, and psychologically timed lures.

The overall objective is not simply to steal data. Iranian espionage seeks to reduce uncertainty for the regime, identify threats before they materialize, monitor opposition and diaspora activity, understand adversary military and diplomatic planning, and build access that can be repurposed during escalation. In Israel, this may mean collecting intelligence on security decision-making, military mobilization, crisis response, and civil resilience. In the United States, it may mean targeting elections, policy elites, defense-adjacent sectors, and critical infrastructure to understand future pressure on Tehran.

In Gulf and Middle Eastern countries, it may mean penetrating telecommunications, ministries, energy firms, and diplomatic networks to monitor regional alignments, sanctions enforcement, normalization efforts, and covert cooperation with Israel or the United States. These examples show that Iranian cyber espionage is not random or purely technical; it is an extension of regime security, regional competition, and strategic warning.

This cyber-enabled intelligence effort should also be understood alongside Iran's repeated attempts over the past few years to recruit Israeli citizens through social media and messaging applications, especially Telegram (Figures 14 and 15). These approaches often begin with anonymous contact, small payments, and seemingly low-risk tasks such as photography, information gathering, propaganda distribution, or logistical errands, before escalating toward more sensitive intelligence or operational assignments.

To date, this effort has had only limited success: Israeli authorities have exposed multiple cases, many recruits appear to have been opportunistic or poorly controlled, and Iran has struggled to convert broad online access into consistently reliable human assets. Nevertheless, the activity is significant because it shows Tehran's willingness to blend cyber access, online influence, criminal-style recruitment, and human intelligence tasking against Israeli society from within.

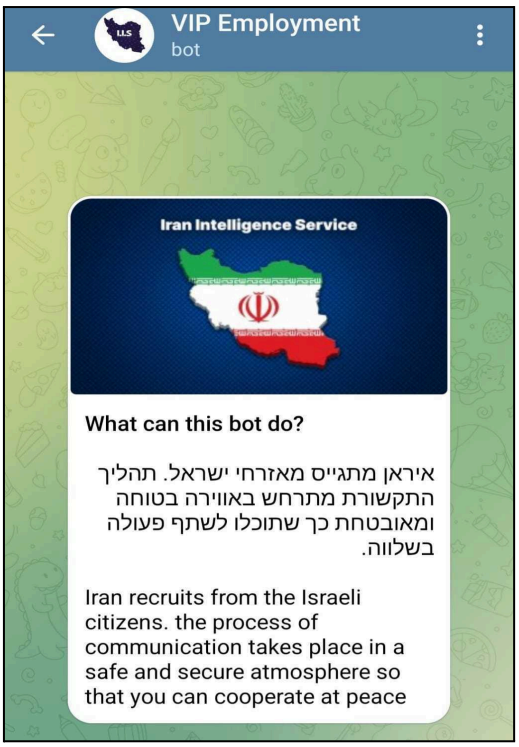


Figure 14 - A message in Hebrew and English from a Telegram bot linked to the Iranian intelligence service for recruiting Israeli citizens



Figure 15 - A private message on Telegram in Hebrew from the Iranian Intelligence Service address to an Israeli citizen

Iran's espionage should therefore not be treated as separate from later coercive operations. Access gained for collection can later support leak operations, intimidation of individuals, proxy targeting, physical surveillance, recruitment attempts, or destructive escalation. For intelligence teams, the key is to distinguish between collection access and activation risk.

Long-term access to a telecom network, cloud tenant, government mailbox, political organization, or individual Israeli contact may initially look like espionage, but in an Iran-related crisis, it can become the foundation for psychological operations, doxing, hostage-related pressure, targeting support, or retaliation.

3.5 Influence and Psychological Operations

Iran's distinctive cyber strength lies in cyber-enabled influence: its ability to convert intrusions, data leaks, fabricated personas, SMS campaigns, website defacements, manipulated media, and exaggerated operational claims into psychological and political pressure. The objective is not always to cause significant technical damage, but to shape how an incident is perceived. Against Israel, Iranian operations seek to convince citizens that the state cannot protect them, that military and civilian institutions are vulnerable, that personal information is exposed, and that political leaders are losing control. Against Western societies, Tehran exploits existing divisions surrounding Israel, Gaza, sanctions, U.S. military involvement, Islamophobia, foreign intervention, and distrust of political institutions.

Microsoft assessed that, following the October 7 attacks, Iranian actors increasingly combined destructive cyber operations or fabricated claims of destructive attacks with coordinated online influence activity. This reflects a central feature of Tehran's operational model: cyber incidents are transformed into narrative events. A limited intrusion can be portrayed as a strategic victory, previously compromised data can be repackaged as a new breach, and even an unsuccessful attack can generate fear when supported by persuasive personas, fabricated evidence, coordinated amplification, and emotionally charged messaging.

This approach remained visible in 2026 through the activity of coordinated pro-Iranian troll and propaganda networks (Figure 16). According to an investigation published by MS NOW, accounts linked to such a network posed as Western journalists, activists, news outlets, and ordinary citizens while disseminating anti-war, anti-Israel, and anti-American narratives across social-media platforms. Rather than openly promoting Iran, these troll accounts attempted to make Tehran-aligned messaging appear to originate organically from Western audiences. By exploiting existing political grievances, conspiracy theories, and polarized public debates, the network sought to increase the credibility and reach of Iranian narratives while concealing their foreign origin.



Figure 16- Now-deleted X account attributed by the Clemson University Media Forensics Hub to an IRGC-linked influence operation. (Source: Clemson University Media Forensics Hub/X.)

The case illustrates an important evolution in Iranian influence operations: Tehran-linked trolls increasingly imitate authentic grassroots communities and independent media voices instead of relying solely on official state outlets or openly pro-regime accounts. Once their narratives are repeated by genuine users, influencers, or political communities, the original Iranian connection becomes more difficult to identify, and the propaganda can acquire greater legitimacy. Actionable indicators include unusually compressed timing between cyberattack claims and propaganda amplification; synchronized cross-posting across Telegram, X, Instagram, Bluesky, and Iranian state media; recently created, repurposed, or coordinated troll accounts claiming Western identities; emotionally charged messaging directed at civilians; fabricated victim testimonies; AI-generated or recycled visual material; and multilingual content in Hebrew, Arabic, English, or other locally relevant languages. Additional warning signs include attempts to connect unverified technical claims to broader narratives of Israeli weakness, Western hypocrisy, government corruption, civilian abandonment, or the legitimacy of the Iranian-led “resistance” axis.

3.6 Disruptive and Destructive Operations

Iran uses disruptive and destructive cyber operations as tools of retaliation, coercion, deterrence, and symbolic punishment. These operations are typically calibrated below the threshold of conventional war, but they can still generate significant political and psychological effects. The CyberAv3ngers campaign against Israeli-made Unitronics programmable logic controllers is a revealing example. CISA reported that IRGC-affiliated actors using the CyberAv3ngers persona targeted and compromised Israeli-made Unitronics Vision Series PLCs, including systems used in U.S. water and wastewater environments.

The targeting logic was not purely technical; it was symbolic. Israeli-made equipment inside Western critical infrastructure provided Tehran with a narrative bridge linking Israel, the United States, and vulnerable civilian services. In 2026, CISA and partner agencies again warned that Iranian-affiliated cyber actors were exploiting internet-connected PLCs and HMIs across U.S. critical infrastructure. The actionable lesson is that Iran often selects targets where political value outweighs technical sophistication: exposed OT, default credentials, Israeli-linked vendors, Jewish institutions, hospitals, municipal services, logistics, and small utilities may be attractive because they provoke fear, generate headlines, and signal deterrence, even when operational impact is limited.

3.7 Integration with Military, Proxy, and Information Operations

Iranian cyber operations are increasingly integrated with the regime's wider doctrine of asymmetric confrontation. Cyber is used alongside missiles, drones, proxy militias, maritime harassment, sanctions evasion, hostage diplomacy, religious-ideological messaging, and information warfare. This means Iranian cyber activity should rarely be interpreted in isolation. During the Israel-Hamas war, Microsoft observed Iranian cyber and influence operations expanding against Israel and perceived supporters of Israel, while the broader "axis of resistance" environment included Hezbollah pressure, Iraqi militia activity, Houthi attacks on shipping, and Iranian diplomatic messaging. Cyber allows Tehran to sustain pressure even when direct kinetic escalation is too risky. It can intimidate civilians, distract decision-makers, impose reputational costs, support proxy narratives, and demonstrate reach into allied societies. From an intelligence perspective, the key is fusion analysis: Iranian cyber escalation should be assessed alongside regional military indicators, proxy rhetoric, Israeli strikes, nuclear negotiations, sanctions enforcement, IRGC casualties, and domestic unrest inside Iran. A spike in phishing against Israeli officials, Gulf ministries, U.S. policy experts, or Jewish organizations may be an early indicator of wider coercive preparation rather than an isolated cyber campaign.

Operational Implications

- Iranian cyber campaigns should be analyzed as multi-domain operations combining espionage, psychological operations, proxy activity, diplomacy, and military pressure.
- Cyber indicators should therefore never be assessed in isolation but fused with geopolitical developments, proxy mobilization, sanctions, military deployments, and regional escalation indicators.
- Organizations that can integrate cyber intelligence with geopolitical analysis will be significantly better positioned to detect Iranian strategic intent.

4. Strategic Targeting

4.1 Israel

Israel is the central target of Iran's cyber strategy because it represents the regime's ideological enemy, principal intelligence rival, military threat, and most useful propaganda adversary. Iranian targeting of Israel serves multiple objectives at once: intelligence collection on military, diplomatic, and technological priorities; intimidation of civilians; disruption of services; exposure of personal data; pressure on political leadership; and support for the "resistance axis" narrative. After October 7, Microsoft reported that Iranian government-aligned actors intensified cyberattacks and influence operations intended to weaken Israel and support Hamas, with activity becoming more targeted and destructive over time. The strategic logic is clear: Iran does not need to defeat Israel militarily in cyberspace to gain value; it needs to create persistent insecurity, amplify domestic polarization, and show that Israeli society is penetrable. Examples include hack-and-leak activity, destructive or ransomware-like claims, attacks against Israeli-linked technology, targeting of universities and civilian organizations, and psychological messaging aimed at hostages' families, soldiers, or the general public. The actionable intelligence focus should be on pre-crisis access to Israeli civilian sectors, repeated Hebrew-language influence assets, cyber personas that synchronize with regional proxy messaging, and targeting of organizations symbolically linked to national resilience: healthcare, education, local government, emergency services, media, and defense-adjacent supply chains.

4.2 The United States and Western Allies

Iran targets the United States and Western allies because they are the principal enablers of sanctions, military containment, Israeli defense, Gulf security, and international pressure against Tehran. Iranian operations against Western targets combine espionage, retaliation, election influence, dissident surveillance, and critical-infrastructure probing. Microsoft assessed that Iran has conducted cyber-enabled influence operations across multiple U.S. election cycles, with activity focused not only on persuasion but also on undermining confidence in election processes and institutions. During the 2024 U.S. election cycle, Iranian-linked APT42 activity was reported against U.S. political campaigns and high-value individuals, using impersonation and phishing tactics. This reflects a broader Iranian doctrine: target the people and institutions that shape policy toward Iran, Israel, sanctions, and regional military posture. Western allies are also attractive when they host Iranian dissidents, enforce sanctions, support Israel, participate in maritime security, or contain Iranian proxies.

Actionable indicators include Iranian-themed phishing against campaign staff, think tanks, former officials, defense contractors, sanctions lawyers, export-control specialists, diaspora media, and Jewish or Israeli-linked organizations. Timing matters: risk rises around elections, military strikes, nuclear negotiations, IRGC designations, sanctions packages, and major Israel-related votes or public controversies.

4.3 Gulf States and Regional Adversaries

Gulf states are strategic targets for Iran because they combine geopolitical rivalry, Western military presence, energy-market importance, intelligence cooperation, and normalization dynamics with Israel. Saudi Arabia, the UAE, Bahrain, and other Gulf actors represent both adversaries and pressure points. Iran’s cyber operations against Gulf targets can support espionage into government decision-making, surveillance of security cooperation with the United States and Israel, collection on energy and finance, and coercive signaling during regional crises. Mandiant’s UNC1860 reporting is especially relevant because the actor’s focus on Middle Eastern telecommunications and government networks suggests a long-term access strategy in precisely the kinds of environments that matter for regional intelligence and crisis leverage. Microsoft has also reported Iranian cyber-enabled influence and disruptive activity affecting regional targets beyond Israel, including entities in Bahrain and the UAE. For Gulf defenders, the intelligence lens should combine cyber and diplomatic context: normalization with Israel, oil-market disputes, U.S. basing decisions, sanctions enforcement, maritime incidents, or public criticism of Tehran can all increase cyber risk. The most sensitive sectors are telecoms, energy, aviation, government services, royal-court or leadership offices, financial institutions, and media outlets.

4.4 Critical Infrastructure and Strategic Industries

Iranian targeting of critical infrastructure and strategic industries is best understood as coercive signaling through vulnerable civilian and economic systems. Tehran is unlikely to seek uncontrolled escalation in most circumstances, but it has shown willingness to probe and disrupt soft targets where attribution ambiguity and symbolic value are high. Water systems, energy, transportation, telecommunications, healthcare, banking, defense supply chains, and industrial control environments are all relevant.

The CyberAv3ngers' targeting of Unitronics PLCs shows how Iran can link technical exposure to political messaging: Israeli-made devices in foreign infrastructure became a symbolic target, allowing the actors to frame the campaign as anti-Israel while affecting U.S. municipal environments. The 2026 CISA advisory on Iranian-affiliated exploitation of internet-connected PLCs and HMIs confirms that this risk did not disappear after the initial Unitronics campaign. Actionably, infrastructure defenders should treat symbolic exposure as a threat factor.

A small utility using Israeli technology, a hospital linked to Jewish institutions, a logistics company serving defense suppliers, or an energy firm supporting Gulf-Israel-Western cooperation may be more attractive than a technically more challenging strategic target. Intelligence requirements should include exposed OT, vendor nationality, remote-access paths, default credentials, public-facing HMIs, crisis relevance, and propaganda value.

4.5 Dissidents, Opposition Networks and Civil Society

Dissidents, opposition networks, diaspora activists, journalists, human-rights defenders, women’s-rights activists, labor organizers, minority groups, and civil-society organizations are priority targets because Iranian cyber operations are inseparable from regime security. The regime uses cyber tools to identify opponents, map networks, monitor communications, intimidate families, expose private information, and disrupt mobilization inside and outside Iran. APT42’s targeting of NGOs, media, academia, legal services, and activists is consistent with this mission. Reuters reported that APT42 operated a fake recruiting business called VIP Human Solutions to identify people in Iran, Syria, and Lebanon who might be willing to share secrets with Israel or Western governments. This example is especially important because it shows Iranian cyber activity blending counterintelligence, deception, recruitment simulation, and potential physical-world consequences. Actionable defensive priorities for civil society include phishing-resistant MFA, strict identity verification before sensitive conversations, compartmentalization of contacts inside Iran, secure device practices for travel, careful handling of invitations from journalists or recruiters, and training around emotional lures.

For intelligence teams, warning indicators include fake HR firms, fake media accounts, suspicious activist-support personas, legal-aid lures, encrypted-messaging approaches, and the collection of personal details that could enable coercion against relatives inside Iran.

Defensive Priorities

Organizations operating within sectors repeatedly targeted by Iranian actors should prioritize:

- Continuous identity monitoring;
- Detection of long-term persistence;
- Third-party and supply-chain risk assessments;
- Executive protection against social engineering;
- Monitoring of hacktivist narratives that may precede or accompany technical operations.

5. Iran Under Cyber Pressure

5.1 Major Operations Against Iran

Iran has also been the target of significant cyber and cyber-enabled operations, which have shaped its threat perception, doctrine, and defensive behavior. The strategic lesson Iran drew from Stuxnet and subsequent operations is that cyber can produce physical, economic, psychological, and legitimacy effects without open war. More recent public examples involve the group Gonjeshke Darande, or Predatory Sparrow, widely described in public reporting as suspected of links to Israel. In June 2025, Reuters reported that the group claimed to have destroyed data at Iran's state-owned Bank Sepah, alleging that the bank supported Iran's military. The following day, Reuters reported an attack on Nobitex, one of Iran's largest cryptocurrency exchanges, in which approximately $90 million was reportedly destroyed rather than monetized. These operations matter because they targeted regime-enabling systems: military finance, sanctions evasion, public banking trust, and crypto-based financial channels. They also mirrored Iran's own cyber-enabled influence model by pairing technical disruption with public messaging. For Tehran, such attacks reinforce the perception that cyber is part of a permanent confrontation with Israel and the West, not an occasional intelligence contest. The exploitation of the BadeSaba prayer application, reportedly manipulated to undermine public trust and turn segments of the Iranian population against the regime, illustrates the willingness of Iran-aligned or Iran-targeting actors to weaponize everyday digital infrastructure for psychological effect (The Soufan Center).

5.2 What Those Operations Revealed

Operations against Iran reveal several structural vulnerabilities: centralized infrastructure, brittle public service systems, politically sensitive financial networks, weaknesses in crisis communication, and a high regime sensitivity to public confidence. Attacks against fuel distribution, rail systems, steel plants, banking, and crypto infrastructure are not only technical events; they expose the regime's dependence on systems that citizens experience directly. Reuters has reported previous Predatory Sparrow-linked activity affecting Iranian fuel stations, including major disruptions in 2021 and 2023, and the 2025 Bank Sepah and Nobitex incidents fit the same strategic pattern. These operations revealed that the Iranian state is vulnerable to psychological pressure when cyber incidents affect daily life, salaries, banking access, transport, or fuel. They also showed that Iran's adversaries understand Tehran's playbook: sabotage, public messaging, and political accusations. The actionable intelligence lesson is that Iran's cyber responses after an attack are often as important as the attack itself. Analysts should monitor internet restrictions, emergency public statements, arrests of alleged insiders, changes in banking access, state-media narratives blaming Israel or the U.S., and retaliatory cyber targeting against symbolic Israeli or Western sectors.

5.3 Iranian Defensive Adaptation

Iranian defensive adaptation has two sides: selective hardening of state and security systems, and stronger control over the domestic information environment. The regime has invested in cyber defense, surveillance, censorship, domestic platforms, traffic filtering, and internet shutdown capabilities because it sees connectivity as both an economic necessity and a political vulnerability. During periods of unrest or conflict, Iran has repeatedly restricted connectivity to limit protest coordination, prevent evidence from reaching the outside world, and reduce foreign intelligence visibility. Recent academic research on Iranian internet shutdowns found evidence of centralized disruption mechanisms, including forwarding-plane null routing while BGP announcements remained stable, which can make shutdowns harder for some outage monitors to detect. This is strategically important: Iran's defensive model is not only about blocking foreign hackers; it is about protecting regime continuity. However, this approach creates trade-offs. Heavy censorship and shutdowns damage economic activity, reveal regime fear, push users toward circumvention tools, and create detectable anomalies. Actionable indicators of defensive adaptation include selective access exemptions for state-linked networks, increased filtering on messaging platforms, unusual routing behavior, VPN-blocking waves, domestic cloud prioritization, emergency telecom orders, and intensified arrests or public attribution campaigns after major cyber incidents.

5.4 Intelligence Opportunities

Iran's cyber ecosystem creates rich intelligence opportunities because it is fragmented, contractor-heavy, politically reactive, and dependent on recurring personas, infrastructure, and proxy relationships. Analysts should look beyond individual indicators of compromise and map relationships among actors, infrastructure, lures, targets, personas, Telegram channels, media amplification, geopolitical timing, and exposed data sources. In this context, leaked databases circulating on cybercriminal forums can sometimes provide valuable intelligence on Iranian security, intelligence, military, contractor, and administrative ecosystems, including names, affiliations, contact details, internal structures, procurement links, or relationships between individuals and institutions. Such material should never be trusted blindly: leaked datasets may be outdated, manipulated, incomplete, fabricated, selectively curated, or mixed with false records (Figures 17, 18, 19 and 20). However, when carefully validated against independent sources, technical telemetry, open-source records, breach context, and known organizational structures, these leaks can significantly enrich actor mapping, support attribution, inform targeting assessments, and enhance understanding of Iran's security and intelligence networks.

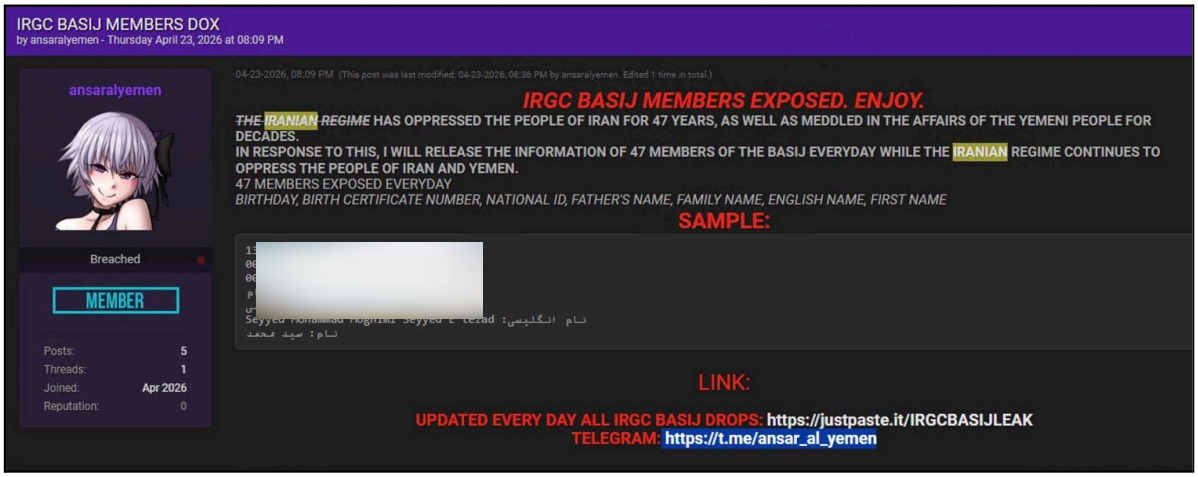


Figure 17 - A threat actor claims to have published a purported database containing information on individuals alleged to be members of Iran's Basij organization. The authenticity and accuracy of the records have not been independently verified.

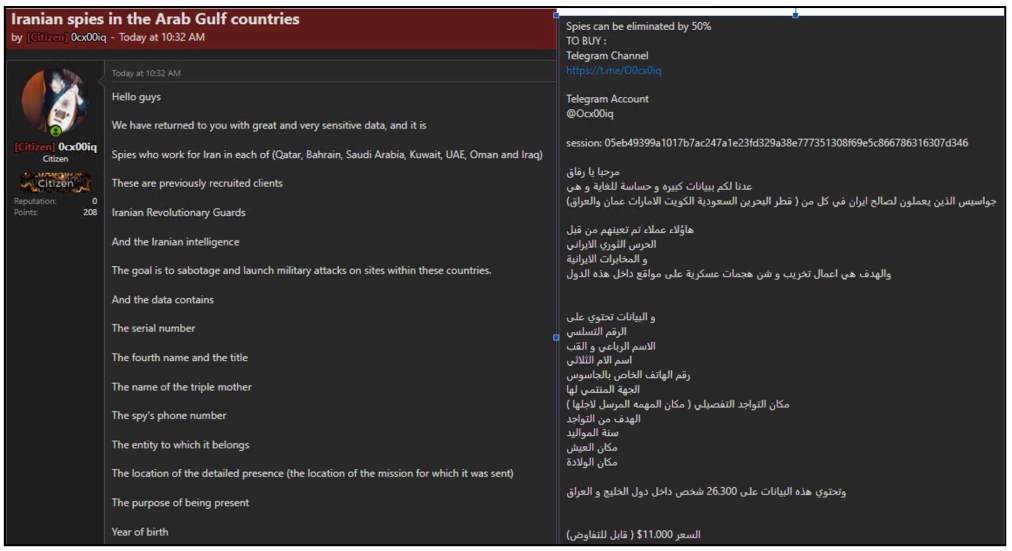


Figure 18 - A threat actor claims to have published a purported database containing information on individuals alleged to be Iranian intelligence officers operating in the Middle East. The identities, affiliations, and authenticity of the records have not been independently verified.

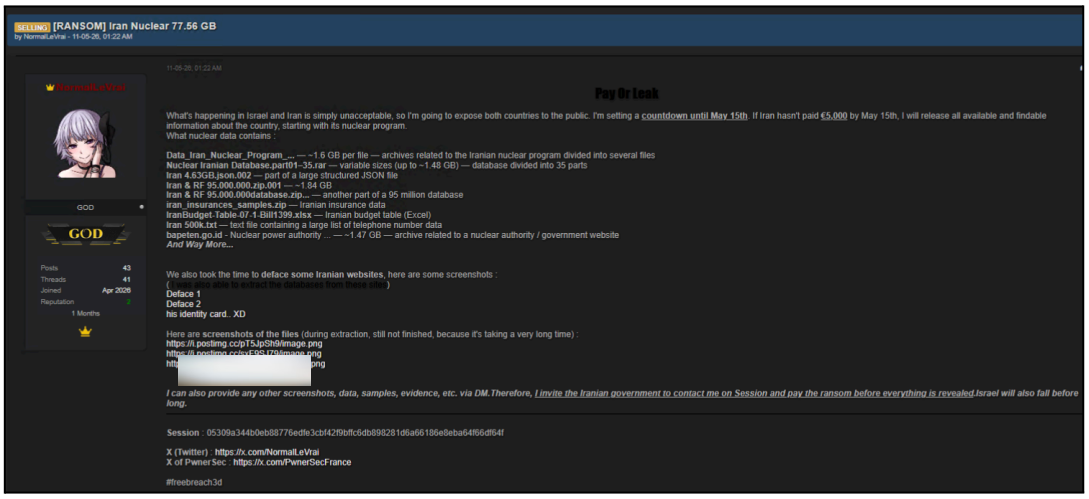


Figure 19 - A threat actor claiming to leak on a cybercrime forum data about Iranian nuclear program on a cybercrime forum

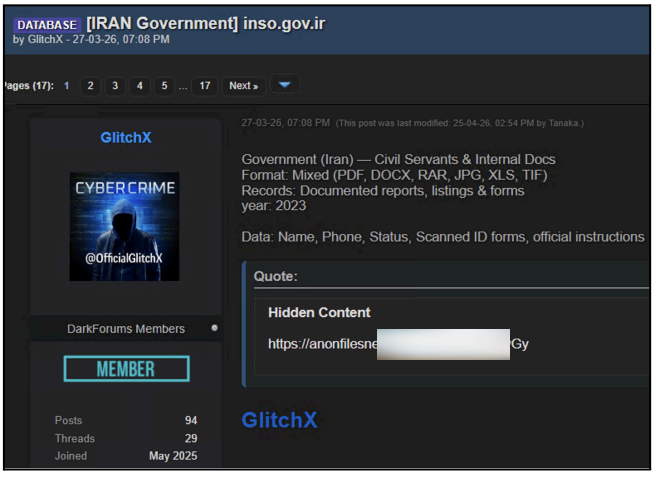


Figure 20 - A threat actor claiming to leak on a cybercrime forum data about the Iranian government

APT42's repeated reliance on social engineering and impersonation provides opportunities to track lure themes, fake identities, credential-harvesting infrastructure, and targeting clusters. UNC1860's role as a likely MOIS-linked access actor suggests another opportunity: identifying infrastructure that supports long-term access across regional telecoms and government networks may reveal broader Iranian operational planning. CyberAv3ngers-style activity shows that symbolic vendor relationships can serve as targeting logic, suggesting that exposure intelligence can help predict future propaganda-driven attacks. Actionable intelligence collection should prioritize seven questions: who developed the access, who used it, who claimed it, who amplified it, what geopolitical event triggered it, what exposed or leaked data can corroborate the picture, and whether the claimed impact is verified, exaggerated, recycled, or fabricated. This framework helps separate Iranian strategic intent from propaganda noise while responsibly exploiting leaked and exposed data as supporting intelligence rather than as standalone truth.

Additionally, anti-regime hacktivist groups such as Lab Dookhtegan have at times disclosed material allegedly linked to Iran's cyber, intelligence, and security apparatus, including information on regime-linked operators, IRGC-affiliated personnel, finance, contractors, tools, infrastructure, and victim profiles (Figures 21 and 22). For analysts, such disclosures can offer a rare window into the internal architecture of Iran's cyber operations and the blurred boundaries between state agencies, security institutions, private vendors, ideological actors, and proxy networks. However, this material should be treated with caution. Anti-regime hacktivist disclosures may be politically motivated, selectively curated, outdated, manipulated, incomplete, or mixed with unverified claims.

Their value lies not in being accepted at face value, but in being carefully validated against independent reporting, technical telemetry, open-source records, sanctions data, corporate registries, infrastructure overlaps, and known patterns of Iranian cyber activity. When properly corroborated, these disclosures can significantly enrich actor mapping, attribution support, contractor identification, targeting assessments, and broader understanding of Iran's security, intelligence, and cyber networks.



Figure 21 - - Lab Dookhtegan claims to have published a purported database of cryptocurrency wallets allegedly associated with the IRGC. The ownership and attribution of the wallets have not been independently verified

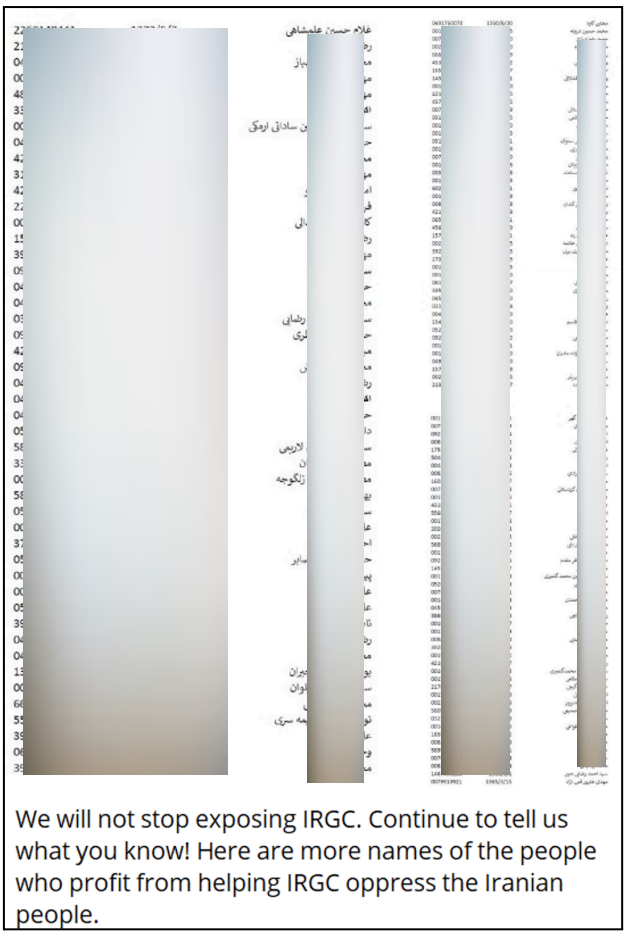


Figure 22 - A threat actor claims on Telegram to have published information on individuals allegedly supporting the IRGC. The identities, affiliations, and authenticity of the records have not been independently verified

Lessons Learned

- Recent operations against Iran demonstrate that cyber and cyber-enabled pressure can disrupt strategically important financial, governmental, and civilian systems while generating wider psychological and political effects.
- At the same time, available evidence suggests that the disruption of individual institutions or infrastructure does not necessarily eliminate capabilities distributed across contractors, external infrastructure, pre-existing access, and semi-autonomous operational networks.
- Future campaigns against Iran should therefore be evaluated not only by immediate operational disruption but by their long-term impact on recruitment, financing, innovation, and command resilience.

6. Strategic Assessment

6.1 Strengths of the Iranian Cyber Model

The strength of Iran's cyber model lies not in technological superiority but in strategic integration. Iran is effective because it uses cyber as a low-cost, deniable, scalable tool of statecraft. It can harass dissidents, collect intelligence, retaliate against adversaries, support proxy narratives, intimidate civilians, and exploit political divisions without immediately triggering conventional retaliation. Canada's National Cyber Threat Assessment 2025–2026 describes Iran as using an aggressive cyber program to coerce, harass, and repress opponents while managing escalation risks, and notes Iran's increasing willingness to conduct disruptive cyberattacks beyond the Middle East. This captures the essence of the model: cyber enables Iran to gain strategic reach despite economic weakness and conventional constraints. Iran's other strength is narrative exploitation. Even when technical effects are limited, Tehran can use personas, leaks, fake claims, and propaganda to magnify perceived impact. This makes Iranian operations particularly dangerous in polarized societies, crisis environments, or sectors with fragile public trust. The actionable assessment is that defenders should measure Iranian cyber risk not only by capability but by political utility. A low-sophistication compromise may still be strategically significant if it supports intimidation, deterrence, or influence.

6.2 Structural Weaknesses

Iran's cyber model also has structural weaknesses. The same decentralization that gives Tehran deniability also creates uneven quality, contractor exposure, operational-security mistakes, duplicated infrastructure, inconsistent tradecraft, and exaggerated claims. Iranian cyber personas often overstate impact, recycle old data, or publish misleading evidence to create psychological effect. Microsoft observed that some early post-October 7 Iranian claims were hasty, chaotic, or false, and often based on outdated material, even as Iranian operations became more coordinated and effective over time.

This creates exploitable seams for defenders and intelligence analysts. Rapid verification, public debunking, and careful impact assessment can reduce the psychological value of Iranian claims. Another weakness is Iran's own vulnerability to the same model it uses against others: its centralized banking, fuel, transport, telecom, and censorship systems are attractive targets for adversaries seeking to undermine regime legitimacy. Iran is also constrained by escalation management. A major destructive attack causing casualties or severe allied economic damage could invite retaliation beyond Tehran's desired threshold. Therefore, Iran often operates in the gray zone, where ambiguity protects it but also limits the scale of what it can safely do.

6.3 Intelligence Gaps

The main intelligence gaps concern command relationships, tasking mechanisms, contractor ecosystems, and the boundary between state-directed, state-tolerated, and opportunistically amplified operations. Public reporting often identifies Iranian-linked behavior with reasonable confidence, but it does not always reveal whether a specific operation was ordered by the IRGC, MOIS, another state body, a contractor, a proxy-aligned group, or a persona acting with loose ideological alignment. This matters because Iranian cyber activity can look more coordinated than it is, or less coordinated than it becomes once state media and proxy networks amplify it. There are also gaps around access depth. A Telegram leak or destructive claim may not prove current access, operational impact, or strategic direction. Analysts should therefore separate four layers of confidence: claimed operation, verified compromise, verified operational effect, and verified state tasking. Another gap is proxy integration. Iran's regional proxies may benefit from Iranian cyber intelligence, narratives, or targeting support, but the degree of direct operational coordination is often difficult to prove publicly. High-value collection would focus on contractor payment flows, tasking channels, shared infrastructure, persona administration, malware development pipelines, and cross-domain synchronization between cyber, media, and military activity.

6.4 Indicators of Strategic Change

Indicators of strategic change in Iran's cyber behavior include a shift from espionage to disruption, from regional targets to global targets, from symbolic defacement to operational impact, and from isolated cyber incidents to synchronized cyber-information-proxy campaigns. Microsoft observed that Iranian operations after October 7 became more targeted, collaborative, and destructive as the conflict progressed. CISA's 2026 warning about Iranian-affiliated exploitation of internet-connected PLCs and HMIs suggests continued interest in operational technology and critical infrastructure exposure.

Other warning indicators include increased targeting of Israeli-linked vendors abroad, phishing against U.S. or European policy communities before sanctions or military decisions, new personas claiming attacks in multiple languages, mass SMS intimidation campaigns, leaks timed to hostage negotiations or military operations, and Iranian state media amplifying technical claims unusually quickly. A particularly important indicator is the "burning" of access. If Iranian actors expose data, deploy wipers, or publicly claim a previously quiet compromise, it may indicate that Tehran has shifted from intelligence collection to coercive signaling. Analysts should also watch for AI-enabled influence improvements, including faster translation, synthetic personas, fake media assets, and automated amplification.

6.5 Future Outlook

Iran will likely continue to expand cyber operations as a strategic equalizer against Israel, the United States, Gulf states, Western allies, dissidents, and critical infrastructure connected to Israeli or Western interests. The most likely future pattern is not a single catastrophic cyber event, but persistent hybrid pressure: credential phishing against high-value individuals, exploitation of exposed infrastructure, long-term access to telecom and government networks, hack-and-leak operations, cyber-enabled influence campaigns, opportunistic OT disruption, and intimidation of diaspora communities. Iran's use of cyber will probably become more integrated with proxy warfare and regional escalation. During future crises involving Gaza, Lebanon, Syria, Iraq, Yemen, the Gulf, or nuclear negotiations, Iranian actors may activate pre-positioned access or launch symbolic attacks against soft targets abroad. The highest-risk scenario is a regional military escalation in which Iran uses cyber to signal retaliation while avoiding direct conventional escalation: exposed PLCs, municipal services, logistics providers, hospitals, financial institutions, Jewish organizations, and Israeli-linked companies abroad would be plausible targets. The most important defensive posture is therefore anticipatory: map symbolic exposure, harden human targets, monitor personal ecosystems, verify claims rapidly, and integrate cyber warning with geopolitical intelligence.

Recommendations for Decision-Makers

- Governments should treat Iranian cyber activity as part of a broader hybrid conflict rather than a standalone technical threat.
- Intelligence organizations should integrate cyber, military, financial, and geopolitical indicators into unified warning models.
- Critical infrastructure operators should assume that espionage access obtained today may become a disruptive capability during future crises.
- Finally, policymakers should expect Iranian cyber strategy to continue evolving toward greater decentralization, deniability, and proxy-enabled operations.

Conclusion

Iran's cyber strategy should be understood as an instrument of regime survival in a period of severe strategic pressure. The regime faces a weakened regional position, intensified sanctions, degraded military and proxy capabilities, repeated attacks on its financial and digital infrastructure, and growing exposure of its internal vulnerabilities. Yet this pressure does not reduce the Iranian cyber threat. It makes cyber more important to Tehran.

A weakened but hard-line Iranian regime is likely to rely even more heavily on cyber because it remains one of the few tools that can deliver intelligence, retaliation, coercion, repression, and psychological effect without requiring direct conventional escalation. For the IRGC, MOIS, and their wider contractor, proxy, and hacktivist ecosystem, cyber offers reach, deniability, and flexibility at a time when Iran's conventional and regional options are increasingly constrained.

The main threat facing the Iranian regime is both external and internal. Externally, Israel, the United States, and allied partners are pressuring Iran's nuclear, military, financial, and cyber infrastructure. Internally, the regime remains vulnerable to economic instability, public distrust, elite insecurity, internet disruptions, and attacks on sensitive systems, including banking, fuel distribution, telecommunications, censorship infrastructure, and cryptocurrency channels. These vulnerabilities show that cyber is not only a weapon for Tehran, but also a critical weakness within the regime itself.

Looking ahead, Iran is likely to adapt rather than retreat. Its cyber activity will probably become more decentralized, deniable, and politically reactive, with greater reliance on semi-official contractors, criminal-adjacent operators, hacktivist personas, proxy-linked actors, and crypto-enabled financing.

The most likely future pattern is sustained hybrid pressure rather than a single catastrophic cyber event: espionage, phishing, hack-and-leak operations, influence campaigns, opportunistic disruption of exposed infrastructure, and intimidation of dissidents or Israeli- and Western-linked targets.

The key analytical point is that Iranian cyber power lies less in technical superiority than in the ability to connect technical access with political timing and psychological effect. A phishing campaign, leaked database, compromised industrial system, or exaggerated hacktivist claim may all serve the same purpose: weakening trust, distracting defenders, signaling retaliation, and projecting regime resilience. Iran's cyber threat will therefore remain significant precisely because the regime is under pressure. Strategic degradation will not eliminate the threat; it will reshape it into a more fragmented, deniable, and hybrid form. Understanding this evolution is essential for anticipating Tehran's future behavior and distinguishing real operational threats from the propaganda noise Iran deliberately creates around its cyber activity.

About the Author



I am a cyber intelligence expert (Crime, Warfare, Terrorism) with over 15 years of experience across academia, high-tech, military, and law enforcement environments. My core expertise includes intelligence strategy, collection, research, and analysis, with a strong specialization in leading cyber intelligence research initiatives and Cyber HUMINT operations targeting criminal and terrorist activity in cyberspace. My research interests center on cybercrime, cyberterrorism, and cyber-geopolitical intelligence. Throughout my career, I have trained numerous civilian analysts, military personnel, and law enforcement officers in cyber intelligence research and operational practices, including work in Deep and Dark Web environments, intelligence collection and analysis, and methodological frameworks.

References

1. Atlantic Council. (2026, January 15). Eight ways AI will shape geopolitics in 2026. Atlantic Council. https://www.atlanticcouncil.org/dispatches/eight-ways-ai-will-shape-geopolitics-in-2026/
2. Canadian Center for Cyber Security. (2024, December 20). Targeted manipulation: Iran's social engineering and spear-phishing campaigns. Government of Canada. https://www.cyber.gc.ca/en/guidance/targeted-manipulation-irans-social-engineering-and-spear-phishing-campaigns
3. Center for Strategic and International Studies. (2026, April 27). The Iranian cyber threat to U.S. critical infrastructure. CSIS. https://www.csis.org/analysis/iranian-cyber-threat-us-critical-infrastructure
4. Check Point Research. (2026, March 1). What defenders need to know about Iran's cyber capabilities. Check Point. https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/
5. ClearSky Cyber Security. (2024, November 12). Iranian "Dream Job" campaign. ClearSky Cyber Security. https://www.clearskysec.com/irdreamjob24/
6. CrowdStrike. (n.d.). Spectral Kitten adversary profile. CrowdStrike. https://www.crowdstrike.com/en-us/adversaries/spectral-kitten/
7. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Department of Defense Cyber Crime Center, & National Security Agency. (2025, June 30). Iranian cyber actors may target vulnerable U.S. networks and entities of interest. CISA. https://www.cisa.gov/resources-tools/resources/iranian-cyber-actors-may-target-vulnerable-us-networks-and-entities-interest
8. Foundation for Defense of Democracies. (2025, June 17). Iran launches counterattacks in cyberspace. FDD. https://www.fdd.org/analysis/2025/06/17/iran-launches-counterattacks-in-cyberspace/
9. Google Cloud Threat Intelligence Group. (2025, November 5). Advances in threat actor usage of AI tools. Google Cloud. https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools
10. Institute for National Security Studies. (2024). The Iranian cyber threat. INSS. https://www.inss.org.il/publication/iranian-cyber/
11. International Institute for Counter-Terrorism. (2026, April 9). From missiles to minds: Iran's influence-driven war strategy. ICT, Reichman University. https://ict.org.il/wp-content/uploads/2026/04/Ben-Yaakov-and-Pack_From-Missiles-to-Minds-Irans-Influence-Driven-War-Strategy_2026_04_09.pdf
12. Israel National Cyber Directorate. (2025, February 4). Technological advancement and evolution of MuddyWater. Government of Israel. https://www.gov.il/en/pages/maddy_water_2024
13. Israel National Cyber Directorate. (2025, December 4). Iranian phishing campaign targets organizational email accounts. Government of Israel. https://www.gov.il/en/pages/muddywater041225
14. Mandiant. (2024, May 1). Uncharmed: Untangling Iran's APT42 operations. Google Cloud Blog.

https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations
15. Microsoft Threat Analysis Center. (2024, February 26). Iran surges cyber-enabled influence operations in support of Hamas. Microsoft Security Insider. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas
16. Office of the Director of National Intelligence. (2026, March 14). Annual Threat Assessment of the U.S. Intelligence Community. ODNI. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf
17. Palo Alto Networks Unit 42. (2025, June 25). Threat brief: Escalation of cyber risk related to Iran. Palo Alto Networks. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2025/
18. Radware. (2025, June 18). Hybrid warfare unfolded: Cyberattacks, hacktivism and disinformation in the 2025 Israel-Iran war. Radware. https://www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/
19. Recorded Future Insikt Group. (2026, June 2). Iran expands Handala brand to physical threats. Recorded Future. https://www.recordedfuture.com/research/iran-handala-physical-threats
20. U.S. Department of Justice. (2024, September 27). Three IRGC cyber actors indicted for “hack-and-leak” operation designed to influence the 2024 U.S. presidential election. https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us
21. Washington Institute for Near East Policy. (2026, May 4). Deniable, disposable, disruptive: Iran’s hybrid warfare in Europe demands a proactive response. https://www.washingtoninstitute.org/policy-analysis/deniable-disposable-disruptive-irans-hybrid-warfare-europe-demands-proactive