The Rise of Iran’s Cyber Capabilities and the Threat to U.S. Critical Infrastructure

Gabrielle Christello

The United States and its allies’ reliance on critical infrastructure to provide necessary functions for their ways of life, to protect their nations, and to maintain strong economies has caught Tehran’s attention. This study examines Iranian cyber-attacks against its neighbors to provide insight into the growing potential for success in future attacks on the United States. This paper examines the evolution of Iran’s cyber threats and its cyber structure within the Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security. The energy and water/wastewater sector case studies highlight vulnerabilities in U.S. critical infrastructure and underscore that small and local utility companies face growing threats from various Iranian state and non-state cyber adversaries. This study stresses the urgent need for Washington to evaluate Tehran’s motivations, opportunities, and capabilities in cyber warfare. Furthermore, it urges enhanced collaboration among stakeholders to fortify critical infrastructure defenses and establish robust cybersecurity standards. It is only a matter of time before Iran launches new cyber phases, including cyber-enabled economic warfare operations and the targeting of vulnerable U.S. and allied computer networks, especially those associated with critical infrastructure.

Introduction

Decades of mounting U.S.-Iran tensions have led to Iran possessing severely limited military capabilities due to the absence of strong state allies, shortage of conventional arms, and lack of nuclear weapons. To improve its ability to challenge and deter the United States, Iran has turned to cyber-enabled espionage, disruptive/destructive infrastructure attacks, and cyber warfare as cost-effective strategies to inflict significant harm. Iran’s tactics using disruptive cyber attacks have become much bolder in the past few years. In response, the United States needs to shore up better cyber defenses as quickly as possible.

Since the 2010 Stuxnet attack – an allegedly joint U.S.-Israeli cyber intelligence operation that deployed the Stuxnet malware against Iran’s nuclear program from 2009 to 2010 – Iran has built up multiple units in the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) that focus on offensive and defensive cyber operations.¹ Further, a 2023 U.S. House Committee on Homeland Security hearing warned that Iran had a “peculiar sense of symmetry” in responding to cyber-attacks.² If Israel, the United States, or its allies were to decide to strike Iran’s networks, Iran could quickly counterstrike by matching the offensive tactics, techniques, and procedures of its adversaries.³ For example, after a retaliatory U.S. military strike in January 2020 that killed IRGC Quds Force Commander, Qasem Soleimani, a former head of the Department of Energy’s Cyber Security Incident Response Team assessed that Iran would be more inclined to target vulnerable U.S. and allied forces’ critical infrastructures due to their potentially catastrophic consequences.⁴

Not only is Iran able to counter-strike its most formidable allies, but since the outbreak of the Israel-Hamas War, Iran’s cyber strategy and tactics have aligned with its military goals. This alignment suggests Tehran has set common objectives for its
domestic stability, territorial integrity, and foreign policy. At the beginning of October 2023, Iran increased its influence operations (IOs) against Israel and leveraged pre-existing access to networks to launch attacks/unleash campaigns.\(^5\) By mid-to-late October, the IRGC launched cyber attacks in tandem with kinetic attacks on international commercial shipping vessels by Iran-backed Houthis.\(^6\) In the span of a year, Iran has demonstrated it can mount four primary cyber-attack tactics: espionage operations, IOs, disruptive/destructive attacks, and mixed attacks (combining some or all the different attacks).\(^7\) This study examines Iran’s cyber attacks against Iran’s neighbors to provide insight into the potential success rate of future attacks in the United States.

In addition to cyber attacks, Iran has also used cyber-enabled economic warfare (CEEW) as a quick, low-stakes option in response to various political and economic conflicts. The term CEEW was first introduced in the 2017 U.S. National Security Strategy to capture adversaries’ use of technology to “weaken our business and our economy.”\(^8\) Tehran has been eyeing the United States and its allies’ reliance on largely privately owned critical infrastructure to service citizens, protect their nations, and maintain strong economies. Most recently, in November 2023, cyber threat intelligence firms, such as Microsoft’s Threat Analysis Center and Mandiant Intelligence, have revealed attempts by the IRGC to launch cyber-attack on U.S. water facilities, confirming growing concern that Iran may be preparing to launch cyber-attacks to disrupt or destroy vulnerable U.S. or allied critical infrastructure networks.\(^9\) Thus, this study examines two case studies that highlight vulnerabilities in the U.S. energy and water/wastewater sectors and underscores the growing threats small and local utility companies face from Iranian state and non-state cyber adversaries. Additionally, this paper argues that Iran’s increasing geopolitical confrontation with Israel and Saudi Arabia suggests Iran may leverage CEEW operations against Western countries as its offensive cyber capabilities improve.

Ultimately, this study forecasts that it is only a matter of time before Iran launches new phases of cyber operations, including CEEW operations and the targeting of vulnerable U.S. and allied computer networks, especially those associated with critical water and energy sectors. Unfortunately, the United States is woefully under-prepared.

**Evolution of the Iranian Cyber Threat**

Iran has a history of cyber retaliation against the United States. In 2010, cybersecurity researchers discovered a computer worm known as Stuxnet had infiltrated computers controlling nuclear centrifuges in Iran.\(^10\) Allegedly a joint effort between the United States and Israel, the code targeted supervisory control and data acquisition (SCADA) systems connected to specific models of programmable logic controllers (PLCs) used for industrial machinery such as uranium enrichment centrifuges.\(^11\) Thus, once the worm took control of the PLCs, it damaged the centrifuges by varying the speed at which they spun, interfering with Iran’s nuclear program.\(^12\) As a result, Iran’s nuclear program was set back by at least two years due to Stuxnet rendering 2,000 centrifuges inoperable.\(^13\) Following the discovery of the Stuxnet worm, the United States experienced an increase in the severity and duration of Iran-affiliated cyber-attacks.\(^14\)

Iran began to expand significantly its offensive and defensive cyber capabilities following the Stuxnet attack. According to a 2012 testimony by Representative Patrick Meehan before the U.S. House of
Representatives, Tehran started to invest USD 1 billion in new cyber warfare technology in 2011.\textsuperscript{15} Offensive and defensive cyber forces since then have resided within the government and military, while other entities like the Mabna Institute in Iran, composed of contractors and university affiliates, have operated more independently.\textsuperscript{16} Iran’s trajectory since 2010 shows how a medium-sized adversary, crippled by sanctions, willingly allocated limited resources to quickly become a cyber power.\textsuperscript{17}

Today, Iranian organizations playing lead roles in cyber operations are either components of the IRGC or belong to varying components of Iran’s elected government, such as the MOIS.\textsuperscript{18} Subordinates of the former often adhere to Iran’s Supreme Leader Ayatollah Ali Khamenei’s orders and interests rather than other government officials.\textsuperscript{19} On the other hand, Esmaeli Khatib leads MOIS, coordinating its intelligence mission with the priorities of the elected government.\textsuperscript{20} The IRGC and MOIS have been reported to lead independent and cooperative operations against perceived Iranian national security threats. Reports by the United States Institute of Peace assess that the IRGC almost exclusively oversees Iran’s offensive cyber activities.\textsuperscript{21} The MOIS also conducts cyber espionage and ransomware attacks on Middle Eastern, European, and North American nations to support Iran’s political goals.\textsuperscript{22} These overlapping operations have complicated U.S. kinetic and cyber attribution by Iranian threat actors to specific organizations within the IRGC or MOIS. Throughout the 2010s, the United States had to aggregate multiple technical, organizational, and personal behavioral data sets for more precise attribution.\textsuperscript{23}

Beyond government-directed cyber operations, scholars suggest the IRGC and MOIS have collaborated with different Iranian threat actor groups and proxies.\textsuperscript{24} However, Tehran has instead characterized the individuals working in collaboration with Iran’s cyber operations as “threat actors,” “state-sponsored,” or “state-aligned,” as a deflection to the direct relationship between the attackers and Tehran.\textsuperscript{25} The relationships between the two ranged from passive support to complete control, with some instances of Tehran orchestrating operations to meet its needs.

To further illustrate the extent of this collaboration, it is critical to understand the specific Advanced Persistent Threat (APT) actors that have been linked to Iran. The various “Kitten” APTs, which an April 2020 report by Insikt Group attributed to Iran, highlight the complexity of the Iranian threat actor network.\textsuperscript{26} "Flying Kitten" gathered intelligence on foreign governments and corporations; "Magic Kitten" targeted domestic dissidents; "Domestic Kitten" targeted dissidents in Iran, the United States, and the United Kingdom; "Charming Kitten" used social networking platforms to reach various targets; "Cutting Kitten" produced website penetration tools; "Nemesis Kitten" conducted malicious network operations and ransomware campaigns; and "Imperial Kitten" targeted Israeli critical infrastructure.

In recent years, Iran’s cyber strategy has become more emboldened, characterized by an increasingly provocative target selection and expanded geopolitical scope. In response to IRGC-inspired attacks against U.S. forces in Northern Iraq and personnel at the U.S. Embassy in Baghdad, President Donald Trump authorized a U.S. military strike on January 3, 2020, that killed Soleimani.\textsuperscript{27} Afterward, the United States issued repeated warnings against potential cyber-attacks from Iran. As anticipated, Iranian hackers of all skill levels accelerated social media disinformation operations,
website defacements, phishing attempts, and network probing. Researchers from RAND assessed that given the scale of the cyber-attacks, Iran may no longer be reluctant to target U.S. and allied forces with wiper attacks, similar to Stuxnet, or look for points of entry into critical infrastructure.

Iran's cyber warfare capabilities have not only grown more sophisticated but also more audacious, as evidenced by their increasing willingness to target a broader range of geopolitical entities. Since Hamas launched attacks on Israel in October 2023, Tehran-aligned actors have initiated a series of cyber-attacks. Their likely intent has been to support Hamas's cause and weaken Israel, its political allies, and business partners. Cyber attacks and IOs are likely to increase as the war continues. Moreover, as of mid-November 2023, Iranian actors had expanded their geographic scope to attack Albania and Bahrain; the U.S. cyber-threat intelligence firm CrowdStrike believed that starting smaller and using cyber operations on regional adversaries could be a testing ground for attacks against future U.S. targets.

**Iran's Cyber-Attack Methods**

Iran has conducted cyber operations to promote its national objectives, the most crucial being the stability and longevity of the Islamic Republic. To achieve such goals, Iran has focused on four primary methods: espionage campaigns, IOs, disruptive/destructive attacks, and mixed attacks (combining some or all methods).

**Espionage Campaigns and Influence Operations**

So far, Iran has more often used IOs and espionage campaigns compared to disruptive/destructive attacks because the former offer a less time-consuming and resource-intensive way to gain maximum exposure to support Tehran’s agenda. Moreover, these methods may serve as a stepping stone to more aggressive operations. Additionally, Microsoft found that cyber-enabled IOs went from one operation every month in 2021 to 11 in October 2023 alone. As the number of IOs rose in the early days of the Israel-Hamas war, researchers observed that these campaigns shifted towards developing targets of interest for destructive cyberattacks, such as data deletion, distributed denial of service, and ransomware.

**Disruptive/Destructive Attacks**

Disruptive/destructive attacks have significantly disrupted the economy and potentially damaged the critical infrastructure of Iran’s neighbors and the United States (e.g., Saudi Aramco in 2012 and denial-of-service attacks on U.S. banks from 2011 to 2013). In December 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an advisory on Iran targeting critical infrastructure, such as transportation, water and wastewater systems, healthcare, and energy pipelines. These attacks were disruptive rather than destructive, probably because Iran’s threat actors lacked Industrial Control System (ICS) specific capabilities. However, the attacks demonstrated that Iran has standard tools to conduct attacks against infrastructure targets and wields a simple, opportunistic approach to information gathering. The targets of these attacks are typically poorly defended small and local utility companies with limited resources to harden their assets. The targeted systems have often not patched severe vulnerabilities listed in Microsoft Exchange. A 2021 CPO Magazine report found that exploited critical infrastructure systems had known vulnerabilities dating back three years. Luckily, as of late 2023, analysis suggests that Iran still lacked the ability to mount...
sophisticated cyber-attacks (such as Stuxnet, the 2021 Colonial Pipeline attack, or Russian actions on Ukraine’s power grid in 2015 and 2022).

Mixed Attacks

As highlighted by the Israel-Hamas war example, Iran has employed a combination of methods for cyber-enabled kinetic attacks on the United States and its allies. Disruptive/destructive cyber operations targeting electricity, water, and fuel infrastructure have reinforced Iran’s geopolitical objectives by incorporating retaliatory messaging to intimidate Israel’s citizens and international supporters and threaten the families of Israel Defense Forces soldiers. Cyber espionage efforts such as phishing campaigns have gathered data and delivered malware to assist with disruptive or destructive cyber operations. Likewise, the number of cyber-attack groups active in Israel rose from nine during the first week of the war to 14 during the second week. Iran is unlikely to expend limited resources on destructive attacks but will maintain the capability to employ them later.

Case Studies: Most Impacted Critical Infrastructure Sectors

Iran’s simple, opportunistic cyber intrusions since 2020 have left threat intelligence firms wondering whether Iran has been simply collecting intelligence and gathering information on conflicts and preparing to launch cyber-attacks to disrupt or destroy vulnerable U.S. or allied networks. So far, the November 2023 water sector cyber attack reigns as Iran’s most successful cyber-attack against the United States. The following case studies hint at Iran’s broader strategic agenda and capabilities to attack U.S. critical infrastructure. Furthermore, the case studies underscore the increasing threats small and local utility companies face from various Iranian state and non-state cyber adversaries.

Energy Sector

After identifying the Stuxnet worm, Iran re-engineered it to use in retaliation against the United States and its allies. The IRGC-affiliated cyberwarfare group called Refined Kitten leveraged Stuxnet to develop the Shamoon malware for multiple operations against Saudi Aramco, a Saudi Arabian state-owned petroleum and natural gas company, in 2012, 2018, and 2020. In 2012, the malware wiped around 30,000 computers and halted operations of the company’s main internal computer networks for 11 days. This attack was Iran’s first publicized destructive cyber operation.

No significant attacks attributed to Iran have happened yet on U.S. energy companies. Although not attributed to Iran, the 2021 Colonial Pipeline ransomware attack exemplifies the impact cyber attacks can have on the U.S. energy sector. Colonial Pipeline controls nearly half of the gasoline, jet fuel, and diesel flowing along the East Coast. This attack caused the utility company to halt operations for five days, skyrocketing gasoline prices. Iran can likely learn from the tactics, techniques, and procedures of this attack to wield a smaller, lower-level opportunistic one of their own. In 2023, Microsoft published a threat assessment on another IRGC-affiliated cyber warfare group, Charming Kitten, and its ability to target critical infrastructure, including energy companies. The group’s capabilities at that time had multiple attack chains and various tools to compromise infrastructures. Charming Kitten’s methodology involved using publicly disclosed code to gain initial access and persist in targeted networks without detection, conducting low-volume phishing
campaigns, and—in some cases—evading detection with customized tools.\textsuperscript{53} This modus operandi and tradecraft are consistent with other IRGC-affiliated cyber actors.

\textit{Water and Wastewater Systems}

From 2018 to 2022, Iran initiated a series of cyber-attacks targeting Israeli water facilities. One attack in 2020 hit small agricultural water facilities near Galilee and infrastructure in central Israel but failed to disrupt Israel’s drinking water.\textsuperscript{54} The attacks likely aimed to trigger a fail-safe, shutting down water pumps. Notably, in other attacks earlier that year, media reports claimed Iran may have intended to override networks to increase chlorine levels in water flowing to residential areas.\textsuperscript{55} Had these efforts been successful, hundreds of people would have been at risk of getting sick, establishing a concerning new precedent for future cyber-attacks. It cannot conclusively be determined if the series of attacks on Israel’s water systems served as a testing ground for Iran’s future cyber-attacks.

Still, these attacks do hint at a broader strategic agenda for Iran. On November 25, 2023, the U.S. government attributed the cyber-attacks on the Municipal Water Authority of Aliquippa, Pennsylvania, and nearly ten other small utilities nationwide to IRGC-affiliated cyber actor Cyber Av3ngers.\textsuperscript{56} By using simple default passwords, attackers likely compromised the Internet-connected industrial control devices made by Israeli company Unitronics to display the message “Down with Israel.”\textsuperscript{57} The breach also resulted in a shutdown of the utility’s automated water pump system, forcing the equipment to operate manually.\textsuperscript{58} CISA concluded that none of the attacks affected operations or access to safe drinking water.\textsuperscript{59} However, the Federal Bureau of Investigation’s section chief of national security cyber operations warned that the access Cyber Av3ngers achieved could lead to deeper network access and cause “more profound cyber-physical effects” going forward.\textsuperscript{60}

\textbf{United States Policy, Legislation, and Recommendations}

Since 2012, Tehran has demonstrated its intent to attack the United States and allies such as Israel and Saudi Arabia through cyber means. In a hearing on the “Iranian Cyber Threat to the U.S. Homeland” in 2012, the Subcommittee on Counterterrorism and Intelligence stated that Washington must prevent Iran from becoming a more capable cyber power.\textsuperscript{61} Yet, in 2018, the Foundation for Defense of Democracies (FDD) emphasized that Washington still had not done enough to understand the Iranian cyber threat, strengthen U.S.-allied defense capabilities, and impose costs on Tehran for its malicious cyber activities.\textsuperscript{62} In September 2023, the Department of Defense’s Cyber Strategy stated that Iran “had not yet demonstrated the ability to conduct significant or sustained malicious cyber activity against the United States.”\textsuperscript{63} Likewise, in November 2023, the news outlet Politico released statements that multiple U.S. federal agencies “stressed that they ha[d] yet to see any intelligence suggesting that Iran is planning an imminent attack on U.S. critical infrastructure.”\textsuperscript{64} Weeks after this article was published, Iran launched its most successful cyber-attack against the United States by targeting the Municipal Water Authority in Pennsylvania. The 2012 House of Representatives hearing addressed the foreseen Iranian cyber threat; 12 years later, the United States remains unprepared to identify, deflect, and outright stop foreseen attacks.

The United States cannot underestimate Iran. As researchers from FDD recommend, the United States must assess Tehran’s
motivation, opportunity, and capabilities to understand the evolving Iranian cyber threat. A key concern is that Tehran’s IOs often lead to destructive operations; these methods are a form of CEEW that weakens strategic relationships between the United States and its allies.

Critical infrastructure is vital to U.S. citizen’s livelihoods and the nation’s economy. However, companies listed under the 16 critical infrastructure sectors have been slow to harden their assets; they place the blame on their complex web of interconnected devices to run operational systems. Given the high stakes, each sector’s resilience requires enhanced collaboration among utility providers, industry-led associations, information-sharing bodies, and U.S. government agencies. Increased communication and awareness will help create best practices, guidance, and standards that raise baseline cybersecurity.

Beyond hardening defenses at home, Washington must send prompt, clear signals to Iran that malicious cyberattacks are unacceptable. Indeed, in February 2024, the U.S. Department of Treasury’s Office of Foreign Assets Control imposed sanctions on six officials of the IRGC-CEC in response to the targeting of critical infrastructure in the United States and other countries. While this action was a necessary step, the attacks on the water facilities happened in November 2023. Responses to cyber-attacks need to be fast; in this case, three months was simply too long.

**Outlook and Conclusion**

Iran’s cyber threat posture will likely slowly but persistently grow in depth and complexity over the next 12 to 24 months. This anticipated growth is rooted in ongoing geopolitical tensions between Iran and its adversaries, notably Western nations and Israel. The persistence of the Israel-Hamas War only adds fuel to this fire, providing Iran with further motivation to enhance its offensive cyber capabilities.

The IRGC and MOIS’s use of cyber personas will likely continue to provide cover for Iran’s IOs and espionage campaigns to gather intelligence and prepare for disruptive attacks. The lack of direct connections between the IRGC’s Cyber Av3ngers and its other cyber threat actors shows an ability to compartmentalize operational techniques, tools, and covers. Moreover, the diversity of cyber actors highlights the value Iran places in leveraging proxies and pro-regime groups for its geopolitical ends.

Iran’s focus on targeting critical infrastructure sectors, evidenced by the recent advancements in attacks on the water/wastewater sector, signals a dangerous escalation in its cyber offensive. The attack on the Municipal Water Authority of Aliquippa, Pennsylvania, ten miles from Beaver Valley Nuclear Power Station, significantly magnifies the threat to the United States. It also highlights foundational vulnerabilities within U.S. critical infrastructure and raises alarming questions about the potential ripple effects on other sectors.

Iran appears to have the necessary cyber capabilities to support its agenda. This study stresses the urgent need for Washington to evaluate Tehran’s motivations, opportunities, and capabilities in cyber warfare. Furthermore, it urges enhanced collaboration among stakeholders to fortify critical infrastructure defenses and establish robust cybersecurity standards. If Washington does not quickly address the advancing threat of Iran’s cyber capabilities, the United States can only hope that the fear
of an overwhelming U.S. response will deter Tehran from escalating the severity of its attacks on critical infrastructure.

About the Author: Gabrielle Christello is a graduate student at Georgetown University’s Walsh School of Foreign Service, pursuing a Master of Arts in Security Studies with a focus on Technology and Security. She holds a Bachelor of Arts in Intelligence Studies and a Bachelor of Science in Cybersecurity from Mercyhurst University. In Fall 2023, she interned as a Cyber and Technology Innovation Intern for the Foundation for Defense of Democracies. Previously, she was a Cyber Specialist at Federal Resources Corporation, consulting small to medium-sized businesses on data breaches and risk assessments. In 2021, she interned at Pfizer, monitoring threats and researching anti-pharma organizations.


Watts, “Iran accelerates cyber ops against Israel.”

Watts, “Iran accelerates cyber ops against Israel.”


Fruhlinger, “Stuxnet Explained.”

Fruhlinger, “Stuxnet Explained.”


Lewis, “Iran and Cyber Power.”


Insikt Group. “Despite Infighting and Volatility.”


Anderson and Sadjadpour, Iran’s Cyber Threat.

Insikt Group. “Despite Infighting and Volatility.”


Fixler, “The Cyber Threat from Iran after the Death of Soleimani.”

Georgetown Security Studies Review 20 Volume 12 | Issue 1
29 Greenberg, “How Iran’s Hackers Might Strike Back.”
30 Watts, “Iran accelerates cyber ops against Israel.”
32 Insikt Group, “Despite Infighting and Volatility.”
34 Watts, “Iran accelerates cyber ops against Israel.”
35 Watts, “Iran accelerates cyber ops against Israel.”
36 Watts, “Iran accelerates cyber ops against Israel.”
37 Theohary, Iranian Offensive Cyber Attack Capabilities.
39 Fixler, “The Dangers of Iran’s Cyber Ambitions.”
41 Fixler, “The Dangers of Iran’s Cyber Ambitions.”
43 Watts, “Iran accelerates cyber ops against Israel.”
45 Joyce and Huntley, “Tool of First Resort.”
46 Fixler, “The Dangers of Iran’s Cyber Ambitions.”
50 “Saudi Oil Producer’s Computers Restored After Virus Attack.”
53 “Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets.”
55 Staff, “Cyber attacks again hit Israel’s water system.”
57 Vazquez and Vicens, “Pennsylvania water facility Hit by Iran-linked Hackers.”
59 “IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors.”
61 Iranian Cyber Threat to the U.S. Homeland.
62 Fixler, “The Dangers of Iran’s Cyber Ambitions.”
Miller, “U.S. Officials Hold their Breath for Iranian Cyberattacks.”
66 Ravich and Fixler, “The Attack on America’s Future.”
69 Fox-Sowell, “Where’s the federal legislation for state water utility cybersecurity?”