Iran Crisis Moves Into Cyberspace

by **Micah Loudermilk (/experts/micah-loudermilk)**

Jul 9, 2019
Also available in
العربية (/ar/policy-analysis/alazmt-alayranyt-tntql-aly-alfda-alsybrany) /
Farsi (/fa/policy-analysis/gstrsh-bhran-ayran-bh-fday-saybry)

ABOUT THE AUTHORS

Micah Loudermilk (/experts/micah-loudermilk)

Micah Loudermilk is a Middle East-based cybersecurity consultant and geopolitical analyst.

Brief Analysis

Iranian cyber actors are showing signs of battlespace preparation, so the United States should heed the lessons of past attacks and bolster its defensive posture.

The growing tensions in the Persian Gulf have recently taken on a cyber dimension, with the United States attacking Iranian military computer systems in response to a drone shootdown and Iranian government hackers reportedly escalating cyber espionage operations targeting U.S. organizations. Tehran has previously retaliated against America in the cyber domain, where low barriers to entry offer a more level playing field—one where the United States is disadvantaged due to its significantly larger attack surface. With Iran showing signs of following this past script, the U.S. government and the private sector need to take appropriate steps to bolster cyber defenses.

REVIEWING IRAN'S RETALIATORY CYBERATTACKS

Whenever Iran has conducted cyber operations in response to past conflicts, tensions, or perceived offenses, it has calibrated them to inflict tangible costs and demonstrate strategic reach while maintaining plausible deniability and avoiding escalation. Notable attacks include the 2012-2013 Operation Ababil campaign against U.S. financial institutions, the 2012 Shamoon attack against oil giant Saudi Aramco, and the 2014 strike against Las Vegas Sands Corporation.

Conducted at a time when Washington was levying additional sanctions on Iran's Central Bank and other entities, Operation Ababil used distributed denial-of-service attacks to disrupt online banking platforms. Although DDoS attacks are rudimentary, Operation Ababil was an effectively targeted campaign that temporarily disrupted some business functions of a critical U.S. economic pillar and caused tens of millions of dollars in damage. Despite claims of responsibility from a hacktivist group called Izz al-Din al-Qassam Cyber Fighters, the attacks were almost certainly sanctioned by the Iranian government.

The Aramco and Las Vegas Sands attacks followed a similar playbook. Although claimed by hacktivist groups with political motivations, both operations were linked to Iran and tied to specific developments that Tehran viewed as threats. Shamoon followed the tightening of U.S. oil sanctions and the discovery of cyber operations against Iran's nuclear infrastructure; the Sands attack came after the company's owner, Republican political donor Sheldon Adelson, advocated a preemptive nuclear attack on Iran.

Despite occurring around the same time, the attacks on Saudi and U.S. firms differed greatly in their destructiveness. Shamoon was one of the most damaging cyberattacks ever reported, destroying more than 30,000 computers, wiping out large portions of Aramco's information technology infrastructure, and crippling the company's business operations. The attack may have been facilitated by an insider who provided network knowledge and privilege escalation, possibly explaining why a Saudi entity was hit in retaliation for U.S. actions.

In contrast, Operation Ababil had significantly lesser effects, temporarily knocking some U.S. banks offline and disrupting customer access. To be sure, the DDoS attacks were large scale—peaking at 70 gigabits per second, significant by 2012 standards. However, they paled in comparison to Shamoon, potentially indicating that Iran made a calculated decision to impose fleeting costs on the United States while avoiding the type of heavy damage that could risk retaliation.

ASSESSING IRAN'S CYBER OPTIONS

Future Iranian cyber operations against the United States would likely take the form of targeted, calibrated attacks against commercial enterprises or critical economic pillars, with the aim of causing damage, inflicting financial costs, and disrupting Americans' lives or business operations. Iran's growing expertise with **wiper attacks (https://www.dhs.gov/cisa/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats)** —coupled with intelligence it has gleaned from ongoing cyber espionage operations—could place a wide range of American entities at risk and challenge Washington's ability to identify likely targets.

The current crisis has already seen evidence of cyber operations on both sides. Last month, the United States launched cyberattacks on Iranian weapons systems after the regime shot down an RQ-4 drone. Cybersecurity companies have also observed battlespace preparations by Iranian cyber actors, which may be a sign of what's to come, as maturing Iranian capabilities and sustained espionage operations point to significant risk exposure for U.S. entities.

In 2012-2014, Iran's cyber capabilities were less developed, so its attacks were typically one-off events rather than sustained campaigns. Today, however, Tehran conducts itself more like China, Russia, and the United States, sustaining long-term reconnaissance and espionage operations that provide it with access and intelligence (e.g., personal data and documents; network and vulnerability maps). Over the past two years, security firms and the U.S. government have identified Iranian cyber espionage operations targeting U.S. government entities, critical infrastructure, military/commercial aviation, manufacturing, and engineering, among other sectors. Iranian hackers have also reportedly targeted the Internet's domain name system and siphoned data from Internet service providers and telecommunications companies that could facilitate future operations.

If Iran escalates to disruptive cyberattacks, they could target the U.S. electrical grid (which it has already probed), water networks (which it has infiltrated), telecommunications systems (which it has mined for data), or even city governments. Last year, two Iranians were indicted by the Justice Department for a ransomware attack against the city of Atlanta, and though they were unaffiliated with the Iranian government, destructive or diversionary ransomware attacks are well within Tehran's capabilities. U.S. allies in the Gulf could likewise find themselves targets of convenience for Iranian hackers, especially Saudi Arabia, which has been regularly attacked or infiltrated since at least 2013.

As the United States used cyber means to respond to a kinetic attack, Iran's leadership may see little reason for strategic restraint in cyberspace. Indeed, the restrained U.S. response may embolden Tehran to move aggressively in that domain, believing Washington has reinforced its reluctance to take action in other military domains. President Trump's oft-repeated skepticism regarding attribution of foreign cyberattacks against America could further incentivize Iranian action, as could his statement suggesting that the drone shootdown may have been a mistake.

MITIGATING U.S. CYBER RISKS

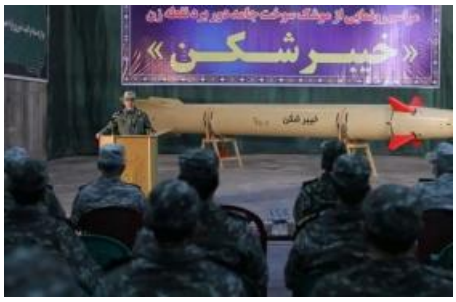
Private-sector entities own and operate most of America's critical infrastructure networks, placing them outside the remit of direct government network defense efforts. Yet policymakers can take several steps to bolster U.S. cyber defenses and potentially dissuade Iranian attacks through shows of force in cyberspace.

For one, sharing more information with potential private-sector targets could help shore up critical infrastructure and assets. At present, intelligence agencies aggressively classify cyber threat information, arguing that this practice is critical to protecting sources, methods, and tools. Yet such policies keep vulnerable entities from obtaining the vital information they need to prevent or mitigate cyberattacks. The Obama administration took **initial steps (https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari)** to address this problem in 2015, but more needs done to either declassify relevant information or provide classified threat briefings to critical infrastructure companies outside the defense sector. With the right intelligence in hand, private entities can defend against attacks—as seen during Operation Ababil, the efforts of Iranian hackers grew increasingly ineffective as banks adapted their defenses.

Additionally, cyber deterrence is difficult when the actors involved are blind regarding U.S. capabilities. This is not to say the United States should reveal its full cyber toolkit. Yet intelligence agencies could take limited steps to demonstrate their reach in cyberspace and give Iran evidence of networked assets they are capable of holding at risk. Similarly, the United States could reach out to Iranian hackers directly via their own networks, showing that their activities are being tracked in realtime. There is precedent for the latter tactic, as U.S. Cyber Command conducted a similar operation against Russian disinformation operatives last year. Such efforts do not require high-profile public action; in fact, quiet displays of power may be more effective at signaling both U.S. capabilities and Washington's genuine interest in de-escalation. Although demonstrations alone are not a long-term solution, they could push Iran to reevaluate its cost-benefit calculus for cyberattacks.

Lastly, policymakers should be careful when drawing redlines regarding retaliation for cyberattacks. The United States does not want Iran to believe that conducting such attacks is cost-free. However, stating a specific redline could limit U.S. response options or create a credibility gap if Washington fails to accurately identify or follow through after an Iranian cyber provocation.

Micah Loudermilk is a Middle East-based cybersecurity consultant and geopolitical analyst. Any opinions expressed here are his own. ❖



BRIEF ANALYSIS

Iran Takes Next Steps on Rocket Technology

Feb 11, 2022

◆

Farzin Nadimi

(/policy-analysis/iran-takes-next-steps-rocket-technology)

BRIEF ANALYSIS

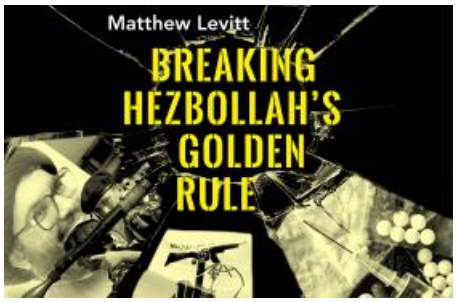
Saudi Arabia Adjusts Its History, Diminishing the Role of Wahhabism

Feb 11, 2022

◆

Simon Henderson

(/policy-analysis/saudi-arabia-adjusts-its-history-diminishing-role-wahhabism)



ARTICLES & TESTIMONY

Podcast: Breaking Hezbollah's Golden Rule

Feb 9, 2022

◆

Matthew Levitt

(/policy-analysis/podcast-breaking-hezbollahs-golden-rule)

TOPICS

Energy & Economics (/policy-analysis/energy-economics)

Gulf & Energy Policy (/policy-analysis/gulf-energy-policy)

Military & Security (/policy-analysis/military-security)

Terrorism (/policy-analysis/terrorism)

REGIONS & COUNTRIES

Iran (/policy-analysis/iran)

Gulf States (/policy-analysis/gulf-states)