The Iranian Cyber Threat

June 2022

UNITED AGAINST NUCLEAR IRAN

UNITED AGAINST NUCLEAR IRAN

Contents

Introduction

In the early morning hours of January 3, 2020, Iran's Islamic Revolutionary Guard Corps (IRGC) Quds Force commander Qassem Soleimani was killed in a U.S. drone strike that targeted his convoy immediately after landing at Baghdad's international airport. Iranian leaders vowed "harsh retaliation" for the attack, but while maintaining a steady pace of provocations targeting the U.S. and its allies, Iran has yet to exact its promised revenge. Following its initial response, a ballistic missile attack on U.S. troops stationed at an Iraqi airbase, Iran's Supreme Leader, Ayatollah Ali Khamenei, warned that the attack was merely a "slap on the face" for the U.S. and vowed to continue to confront the U.S. until Iran has expelled its influence from the region. As Iran approached the one-year anniversary of Soleimani's assassination, Khamenei warned the U.S. in December 2020 that Iran remains bent on revenge, stating, "Both those who ordered his assassination and the assassins themselves should know that we will take our revenge in due time – at the proper time."

Cyber Retaliation

The U.S. national security apparatus has cautioned that one avenue for retaliation Iran is likely to pursue

is launching offensive cyber attacks targeting the U.S. public and private sectors. The day after Soleimani's killing, the Department of Homeland Security (DHS) issued a bulletin warning that while it did not have information about an imminent attack, "Iran maintains a robust cyber program and can execute cyber attacks against the United States. Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure in the United States." Such an attack could further "come with little or no warning." Several days later, the Cybersecurity and Infrastructure Security Agency (CISA) within DHS issued an alert to stakeholders in the U.S. cybersecurity community recommending a heightened state of awareness and increased organizational vigilance, urging cybersecurity personnel to immediately flag "any known Iranian indicators of compromise and tactics, techniques, and procedures."

The FBI similarly issued an advisory, obtained by Cyberscoop, to U.S. companies on January 9, 2020, assessing that Iranian hackers could use "a range of computer network operations against U.S.-based networks in retaliation for last week's strikes against Iranian military leadership." The FBI advisory noted that there had been an uptick in Iranian "cyber reconnaissance activity" since the Soleimani killing and offered technical advice to companies on thwarting Iranian efforts to exploit vulnerabilities in virtual private network (VPN) applications, which Iran has historically used to gain a foothold in computer networks allowing it to monitor, exfiltrate, and potentially destroy sensitive data.

The FBI and DHS advisories echoed assessments issued by the U.S. intelligence community for several years, warning of Iran's determination and ability to launch offensive cyber attacks against the U.S. and its allies. The 2018 Worldwide Threat Assessment of the U.S. Intelligence Community concluded that Iran "will continue working to penetrate U.S. and Allied networks for espionage and to position itself for potential future cyber attacks." The assessment further warned that Iran is growing increasingly aggressive and will only be further emboldened absent significant push back against its malign cyber activities. According to the assessment, "The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners." The 2019 Worldwide Threat Assessment noted that the Iranian cyber threat had entered a new phase, with Iran increasingly focused on deploying "cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries." At this point, Iranian cyber attacks are capable of "localized, temporary disruptive effects – such as disrupting a large company's corporate networks for days to weeks." The 2020 Worldwide Threat Assessment found that the Iranian cyber threat has advanced further, as Iran has now acquired "the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities."

The mounting concerns over an Iranian cyber attack reflect the considerable investment Iran has made in advancing its cyber warfare capabilities over the past decade. In 2010, over 15 Iranian nuclear facilities were targeted by the Stuxnet computer virus, a worm jointly developed by the U.S. and Israel that destroyed nearly 1000 centrifuges. The attack exposed the weakness of Iran's cyber defenses, leading Iran to accelerate the advancement of offensive and defensive cyber warfare capabilities. By March 2012, Iran created a "cyber command" known as the Supreme Council of Cyberspace, comprised of senior military and intelligence officials. The council acts as a unified command tasked with coordinating Iran's cybersecurity and plotting out of offensive and retaliatory cyber operations.

Iran's National Security Strategy

Iran's investment in developing its cyberwarfare capabilities fits into Iran's national security strategy that relies extensively on asymmetric warfare. Iran has honed this strategy since the end of the 1980- 1988 Iran-Iraq War, a war that cost Iran over 300,000 lives and devastated the Islamic Republic's economy and infrastructure. The war shaped the worldview of the network of IRGC officers who served in the war and who form the core of Iran's military elite to this day, hardening their enmity toward the U.S. and inculcating an aversion to head-to-head combat. As a result, Iran sought asymmetric response capabilities that would enable it to prevail in conflict with stronger powers.

As a revisionist regional power, the Islamic Republic of Iran's hegemonic strategy is predicated on supplanting Western influence throughout the Middle East and spreading its Islamic revolutionary doctrine. Iran is hamstrung in this effort by its inferior conventional military forces compared to its adversaries, the U.S. and its Middle Eastern allies. Iran's annual military budget is estimated to be below $20 billion per year, which is dwarfed by Saudi Arabia, the world's number three annual defense spender at $67.6 billion per year. While Iran's defense spending is roughly in league with other adversaries such as the United Arab Emirates and Israel, Iran's military is qualitatively inferior due to procurement issues, as Iran is subject to a U.N. arms embargo.

Despite these structural disadvantages, Iran has succeeded in establishing pockets of political, military, and diplomatic influence in neighboring countries instead of relying on asymmetric means. Iran has, for instance, cultivated ties with militias and terrorist organizations to anchor loyal proxies in and destabilize neighboring states, giving it outsized influence in Lebanon, Iraq, Syria, and Yemen. Similarly, it has amassed the Middle East's largest and most diverse ballistic missile arsenal and developed an advanced drone program, mitigating its air force's lack of a long-range strike capability. Ultimately, Iran seeks to leverage its asymmetric warfare strategy to increase the costs to the U.S. of maintaining its military presence and influence in the region with an eye toward driving it out.

Iran's development of cyberwarfare capabilities makes for a potent addition to its asymmetric toolkit that gives Iran an additional, low-cost means beyond its limited conventional capabilities to conduct espionage on and strike stronger adversaries in furtherance of its foreign policy and national security objectives. Despite its aggressive malign regional conduct, Iran is a risk-averse actor that seeks to avoid direct combat against conventionally superior adversaries. Cyber attacks enable Iran – either offensively or in retaliation – to inflict serious economic and national security costs in a manner that typically offers an element of attribution with deniability as to the origin of the attack and reduces the likelihood of a kinetic response.

The cyberwarfare domain is additionally appealing as it offers a relatively even playing field, and Iran has been a pioneer in demonstrating the power of weaker actors to confront superpowers. Iran is a second-tier cyber threat with indigenous capabilities that match North Korea, lagging behind the biggest threat actors, Russia and China. As such, Iran may be capable but would have difficulty executing on its own major cyber attacks against the highest-value targets in the U.S., the federal government, the military, the largest banks and corporations, and the most critical industrial control systems – water systems, the electric grid, transit systems, oil refineries, manufacturing, and other major infrastructure. More worryingly, there are multitudes of soft targets, such as state and local governments, small banks, and critical infrastructure whose networks contain vulnerabilities that Iran can and has sought to exploit. Complicating matters, Iran could potentially buy the services of first-rank skilled actors on the dark web if

it sought to attack the highest-value targets in the U.S. in the short term. This would bring Iran better technological skills and the imprimatur of a foreign hacker in prospective attacks, masking Iran's involvement.

Laying the Groundwork

According to the U.S. government and cybersecurity experts, Iran has indeed been laying the groundwork for major cyber attacks on high-value targets, especially industrial control systems. At the 2018 Aspen Security Forum, U.S. officials warned that "Iran is making preparations that would enable denial-of-service attacks against thousands of electric grids, water plants, and health care and technology companies in the U.S., Germany, the U.K., and other countries in Europe and the Middle East." James Lewis, a former State Department cybersecurity and intelligence official, further added, "The Iranians have been doing these types of probes for years now — mapping out the networks of critical infrastructure to find potential vulnerabilities." In October 2019, a cybersecurity researcher from the Netherlands identified 26,000 industrial control systems across the United States that are largely unguarded and vulnerable to a cyber attack.

The U.S. and Iran have been in a state of heightened tensions since the Trump administration withdrew from the Iran nuclear deal in May 2018 and imposed a "maximum pressure" campaign. While the Biden administration has made a "compliance for compliance" restoration of the JCPOA one of its top foreign policy priorities, Iran has continued escalating its provocations as part of its strategy to increase its negotiating leverage, commencing enrichment of uranium to up to 60% purity, continuing to advance its ballistic missile program, targeting commercial shipping and energy infrastructure in the Persian Gulf region, and launching rocket attacks through its proxies against the U.S. military presence in Iraq.

As part of its campaign to pressure the U.S. to provide up-front sanctions relief ahead of resumed nuclear negotiations and its broad resistance to U.S. influence in the Middle East, offensive cyber attacks are a potential avenue that Iran is likely to pursue, especially given its heavy investment in the domain and multitude of vulnerable nodes it can target. An attack targeting physical infrastructure would mark a dramatic escalation for Iran and would likely trigger heavy reprisals, which has largely prevented them from attempting such attacks thus far. Still, the concern in the national security and intelligence communities that Iran has attained such capabilities highlights the need for vigilance and for public and private sector stakeholders to harden their cyber defenses.

This resource contains two sections. The first focuses on the structure of Iran's cyber infrastructure—offensive and defensive. The second analyzes the Islamic Republic's cyber methods and modus operandi, profiling the kinds of operations it has employed in recent decades. The resource concludes with recommendations for how to best tackle the Iranian cyber threat.

Structure

The Iranian regime has three primary objectives in the cyberwarfare arena: defending its critical infrastructure and sensitive data from cyber attacks, monitoring and responding to online activity within the country, and carrying out offensive cyber operations. The 2009 Green Movement protests laid the groundwork, leading Iran's security forces to boost their hacking capabilities in order to bolster domestic

surveillance and control of cyberspace. The 2010 Stuxnet attack on Iran's nuclear program served as a catalyst for Iran to expand on these initial advances, and in a short amount of time, to rapidly develop its offensive and defensive cyber capabilities.

Defense

In July 2011, the regime allocated $1 billion to boost the country's cyber capabilities, investing in new offensive and defensive technologies and the recruitment and training of a cadre of cyber experts. In tandem, Iran stood up a variety of domestic agencies tasked with administering cyberspace affairs. In March 2012, Supreme Leader Khamenei announced the formation of Iran's Supreme Council on Cyberspace, unifying the country's various cyberspace organs under a single command. The Supreme Council is tasked with setting Iran's cyberspace policies and strategies from on high, while the somewhat overlapping organizations under it follow its directives. According to the BBC Persian, "This council comprises the highest-level Iranian authorities such as the president, the heads of the judicial power and the parliament, the head of the state-run radio-television, the commanders-in-chief of the IRGC and the police, the ministers of Intelligence, Telecommunication, Culture, Science, etc."

The main Iranian body tasked with cyber defense is the Cyber Defense Command, which operates under the aegis of Iran's Passive Defense Organization, and is itself a subdivision of the Armed Forces General Staff and is overseen by a committee headed by the chief of staff of Iran's Armed Forces. The Passive Defense Organization is charged with coordinating the response of agencies throughout the government to mitigate damage to critical infrastructure and sensitive facilities, non-kinetic responses to military attacks on Iran, and combatting internal dissent in cyberspace. The dedicated Cyber Defense Command was established in November 2010 in response to the Stuxnet attack, and is tasked with crafting defensive cyber doctrine and repelling or mitigating the damage of cyber attacks targeting Iran.

Offense

The IRGC's *basij* and intelligence organization are the primary cyber threat actors behind Iran's offensive cyber operations, although it must be noted that the *basij*'s cyber forces are highly unprofessional. The *basij* has used its ties to universities and seminaries to recruit a volunteer "cyber army," the majority of whose operations consist of online posts and replies in favor of the regime. The *basij* recruits have also engaged in lower-level hacking and infiltration of websites and emails, although some of the most promising recruits are reportedly trained by IRGC operatives to assist in more complex operations.

The IRGC intelligence organization, meanwhile, is the actor behind Iran's most significant and destructive offensive cyber operations, and is believed to be behind attacks targeting computer networks in the U.S., Israel, Europe, Saudi Arabia, and other Gulf states. Officially, the IRGC denies that it engages in offensive cyber operations, claiming that the thousands of "cyber warriors" it purports to have at its disposal engage only in dissemination of online pro-regime propaganda. The cyber arena allows Iran to use proxies and cutouts to carry out its operations, and these actors remain at arms- length from the official state.

The earliest Iranian-attributed offensive cyber operations were carried out by a group calling itself the Iranian Cyber Army, a collection of ostensibly independent hackers alleged to be sponsored by the IRGC. Later on, as the Iranian Cyber Army faded from the scene, additional hacking collectives emerged with

names such as the Izz ad-Din al-Qassam Cyber Fighters, APT 33 (aka Elfin, Refined Kitten, Holmium), Phosphorous (aka APT 35, Charming Kitten, Ajax Security), and OilRIg. These collectives typically employ a "scattered set of independent contractors who mix security work, criminal fraud, and more banal software development," according to the Carnegie Endowment report. Major Iranian cyber attacks sometimes would employ contractors from multiple institutions, including IT firms and universities, carrying out different phases of the campaign, with the IRGC believed to be the bankroller and coordinator.

The Iranian cyber threat is complex to track, as campaigns and new threat groups disappear as quickly as they emerge, particularly when detection of malign cyber activities is suspected. This shows a lack of sophistication on the part of Iranian cyber forces as state-aligned cyber forces in more advanced countries are typically permanent fixtures, but also provides a strategic advantage and helps Iran maintain plausible deniability. However, there do appear to be commonalities in the tactics, software, and lines of codes used tying these groups together, with evidence ultimately leading back to the IRGC.

U.S. indictments against Iranians engaged in cyber sabotage and espionage have revealed operations that "required costly infrastructure, including dedicated servers and dozens of domain names, in addition to personnel time," indicating the involvement of Iran's intelligence services. The level of involvement of the IRGC in the planning and execution of cyber attacks is often difficult to ascertain, but the objectives of Iran's cyber threat actors typically advance the foreign policy and national security objectives of the Iranian regime.

History of Iranian Cyber Attacks and Incidents

The asymmetric nature of the cyberwarfare domain has enabled Iran to carry out the most sophisticated and costly cyber attacks in the history of the internet age. As Iran's capabilities have expanded, driven by increased investment over the past decade since the Stuxnet attack on Iran's nuclear facilities, Iran's malign activities in the offensive cyber realm have evolved and advanced. Iran has kept up a steady drumbeat of lower-level attacks against the U.S., its allies, and regime opponents at home and abroad, some successful and others thwarted. The most common publicly-known attacks include simple website defacements, online disinformation campaigns to push pro-Iranian regime and anti-U.S. narratives, distributed denial of service (DDoS) attacks, and theft of personally identifiable information and intellectual property. At times, Iran has pushed the envelope launching attacks using destructive wiper malware, crippling entire computer networks.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) within DHS notes that according to open-source reporting, numerous offensive cyber operations have been attributed or are alleged to be the work of the Iranian government, or at least Iranian actors working in conjunction with or with the approval of the regime. According to CISA, Iran's cyber attacks have targeted sectors including "financial services, energy, government facilities, chemical, healthcare, critical manufacturing, communications, and the defense industrial base." While many Iranian attacks are destructive in nature, others are conducted for purposes of espionage and intellectual property theft, designed to give Iran insights into its adversaries' strategic planning or to improve its own industrial or military capabilities in the face of sanctions.

The Attacks

The following accounting of the most significant Iranian cyber attacks, either attempted or completed, shows the evolution in Iran's increasingly sophisticated and bold cyberwarfare activities. The incidents recounted also give an indication of how cyberwarfare fits into Iranian statecraft and national security strategy. Even at times of relative stability or low tensions, Iran has still been active in the cyber domain. Iran's cyber activities tend to escalate in response to provocations and heightened tensions. On occasion, Iran has resorted to crude, quick strikes when it has sought to immediately respond to a provocation, such as the imposition of new sanctions. Other Iranian malign cyber activities, particularly those of its primary hacker collectives, demonstrated slow and methodical planning involving the strategic selection of targets, the development of custom malware, and protracted periods of infiltration before the deployment of its cyberweapons.

According to the Carnegie Endowment report , "While the Iranian hacking scene emerged in the early 2000s, there is little evidence of state-aligned cyber activities before 2007." The earliest impetus for malign offensive Iranian cyber activities was the June 2009 Iranian presidential election, which witnessed the re-election of Mahmoud Ahmadinejad amid widespread, credible allegations of fraud by Iran's revolutionary regime. The contested election spurred the rise of the opposition Green Movement and marked a perilous period for Iran's government as its legitimacy increasingly came into question.

Iranian Cyber Army

The internet and social media were central to the Green Movement's mass mobilization efforts, and the Iranian government subsequently went to war against websites and platforms affiliated with the opposition movement or seen as enabling their ongoing communications and supporting their messaging. Between December 2009 and mid-2011, a group calling itself the Iranian Cyber Army launched a campaign of website defacements targeting sites seen as sympathetic to the Green Movement, replacing their homepages with graphics and messages in support of the Iranian regime. The Iranian Cyber Army is nominally a collective of independent hackers whose aims and ideology are in lockstep with the Iranian governments, but given the regime's tight controls over the cyber realm, its activities are believed to be overseen by the IRGC's intelligence apparatus.

Among the group's targets was Twitter, whose homepage the group hacked and defaced in December 2009 with pro-Iranian and anti-U.S. messages. A month later, the group carried out a similar attack on China's primary search engine, Baidu. In February 2011, the Iranian Cyber Army claimed credit for a similar attack on the Voice of America's homepage. Other targets included websites and news outlets affiliated with Iranian opposition elements, including Mowjcamp, Radio Zamaneh, Amir Kabir Newsletter, Jaras, and the MOBY Group.

The Iranian Cyber Army's attacks during this phase were primitive, but still potentially destructive. They did not rely on technical breaches of infrastructure at the sites themselves, but on social engineering that exploited weaknesses at the sites' domain registrars, the companies that host the websites. The Iranian Cyber Army's attacks, known as domain name systems (DNS) attacks, involved impersonating employees at the respective websites with requisite levels of access to the site's control panels, contacting the domain registrar in order to obtain passwords, and then hijacking pages and redirecting site traffic to pages containing the pro-Iranian propaganda. Obtaining DNS access would enable hackers to control

websites' sensitive data, but in these instances, it appears no data was compromised and the attacks merely hijacked control of the sites for limited periods for propagandistic purposes.

Iranian Hacker(s)

Following the 2010 Stuxnet attack on Iran's nuclear program, Iran rapidly began investing in and improving its offensive cyberwarfare capabilities, which ushered in increasingly sophisticated attacks. In September 2011, an Iranian hacker (or hackers) claimed credit for an attack that compromised the Dutch certificate authority, DigiNotar, and issued fake security certificates, which communicate to your web browser that the site you are visiting is the site you intended to visit. The hack effectively gave Iran the ability to access the Gmail accounts and spy on the encrypted communications of 300,000 Iranian users. The attack was claimed by a hacker who claimed to have acted alone and who chose to help his government monitor the communications of his fellow citizens, yet it appears that Iranian intelligence was involved as well. The UK Government Communications Headquarters (GCHQ) provided a post-mortem account of the DigiNotar event in which it alleged that an "Iranian intelligence agency added a specific rule in an internet router that forced Google's traffic through an alternative route inside the country."

Having cut their teeth responding to the internal threats to national cohesion and stability represented by the Green Movement, Iran's cyber threat actors would go on to adapt an offensive cyber posture geared toward confronting the regime's internal and foreign adversaries concurrently. The same infrastructure and cyberweaponry used against the Iranian opposition would also be turned against the U.S. and its allies.

Madi

The earliest incidents of major external Iranian cyber attacks were initially reported in the summer of 2012. In July, 2012, security firms Kaspersky Lab and Seculert uncovered an Iranian cyber espionage campaign, relying on spyware called Madi, ongoing since December 2011 that affected 800 victims over the course of a year. The campaign primarily targeted business executives in the fields of critical infrastructure and financial services, as well as Middle Eastern government officials and embassy staff. Of those targeted, 387 were in Iran itself, 54 in Israel, and the rest scattered around the Middle East and Afghanistan. The campaign relied on crude spear-phishing tactics. Those affected clicked on PDF or Microsoft PowerPoint attachments or links to news articles. Once the users downloaded the corrupted files, a Trojan spying software called Madi would be secretly loaded onto their computers. Remote attackers would then be able "to swipe sensitive files from infected Windows computers, monitor email and instant messages exchanges, record audio, log keystrokes, and take screenshots of victims' activities." Based on the code used, the researchers who uncovered the Madi campaign characterized the hackers' tradecraft as "amateurish and rudimentary," yet effective.

Major Attacks on U.S. Banks and Casino

Iran followed up the Madi campaign with a major offensive cyber operation targeting the U.S. banking sector, heralding the Islamic Republic's arrival as a major cyberwarfare actor. Beginning in December 2011, an Iranian hacking group calling itself the Izz ad-Din al-Qassam Cyber Fighters began laying the groundwork for a series of Dedicated Denial of Service (DDoS) attacks against U.S. financial institutions. In

March 2016, the U.S. Department of Justice unsealed an indictment against "seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps," responsible for carrying out the series of attacks. The indictment offered a rare glimpse into Iran's modus operandi with regard to cyber attacks, demonstrating the IRGC's penchant for using multiple contractors each with their own set of objectives in an attack. According to a leaked briefing document of the National Security Agency obtained by the Intercept, the agency picked up signals intelligence stating explicitly that the campaign was conducted to retaliate against the U.S.'s cyber attacks on Iran's nuclear facilities, and that senior officials in the Iranian regime were aware of the attack.

The first phase of the campaign, named Operation Ababil, involved the culprits exploiting vulnerabilities in the software of thousands of websites in order pool bandwidth, which it then used to overwhelm their targets. After a few sporadic DDoS attacks, in September 2012, the campaign began in earnest and would continue in phases until July 2013, by which time, the major players in the financial sector had shored up their defenses, leading to the campaign fading away. Ultimately, the culprits hacked into the servers of 46 primarily financial institutions, including Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T and HSBC, deluging them with up to 140 gigabits of data per second, far exceeding their capacity and thereby denying customers from logging into their online bank accounts. The group's DDoS attacks occurred in waves on 176 distinct days, costing the affected institutions tens of millions of dollars in remediation costs as they worked to counter the attacks.

Following the DDoS campaign against U.S. banks, Iranian "hacktivists" carried out a data deletion attack against the network of a Las Vegas casino owned by Sheldon Adelson, an outspoken opponent of Iran's nuclear program. Personal computers and servers operating on the casino's network shut down and had their hard drives wiped clean, disrupting the casino's operations. The attack destroyed three-quarters of the casino's servers and the costs of data recovery and rebuilding IT infrastructure were estimated at $40 million. Cyber security researchers determined based on the scale and sophistication that the attack could not have been achieved without government knowledge or backing.

New York Dam

One of the co-conspirators in Operation Ababil was additionally indicted for allegedly hacking into the control system of a dam in upstate New York between August 28 and September 21, 2013. The level of access he had obtained would have allowed him to operate the dam's sluice gate, responsible for regulating water levels and flow rate. However, the dam's sluice gate had been manually disconnected at the time of the intrusion for maintenance. This incident was alarming, as it demonstrates Iran's ability and desire to access industrial control systems, as well as the vulnerabilities posed by the thousands of soft sites around the country that can potentially be manipulated, leading to potential loss of life.

Shamoon

Iran has at times directed cyber operations against U.S. allies as well, with the most significant attacks targeting Saudi Arabia. In addition to being in a state of cold war with Saudi Arabia for regional dominance, targeting American allies is a way for Iran to strike an indirect blow against U.S. interests that is less likely to provoke an American response. In 2012 and then again in late 2016 and early 2017, Iranian-origin malware called Shamoon targeted the Saudi Arabian government and private sector. The

Shamoon malware works by overwriting computers' master book record, making it impossible for them to start back up.

The initial 2012 Shamoon attack targeted Saudi Aramco, a company responsible for 10% of the world's oil supply at the time. The groundwork for the attack was laid mid-year, when an Aramco computer technician opened a spam email and clicked on a malicious link. On August 15, 2012, the actual cyber attack commenced, and the malware began deleting and overwriting the data on around 30,000 computers. Affected computers were effectively "bricked," and reportedly displayed images of a burning American flag. The attacks were timed to coincide with Ramadan, when most workers would be absent to allow the malware the maximum time to work unimpeded. The malware only infiltrated office computers and did not impact systems dealing with technical operations. Still, it grounded services to a halt, as office workers resorted to communications with typewriters and fax machines and gasoline refill trucks were turned away with no way to process payments. To mitigate the damage, Aramco purchased 50,000 hard drives, paying higher prices to cut the line and buy all the hard drives on the manufacturing line at several Southeast Asian factories.

The U.S. intelligence community has attributed the Aramco attack to Iran. A group calling itself the Cutting Sword of Justice claimed responsibility for the attack, posting a missive online that blamed the "Al-Saud corrupt regime" for using its oil resources to fund "crimes and atrocities" in Middle Eastern countries. The attack was believed to be retaliation for a similar attack that targeted Iran's oil ministry and National Iranian Oil Company in April 2012. That attack used malware called Wiper to delete hard drives before vanishing. The Shamoon attack demonstrated an Iranian capability to learn from attacks against it and weaponize tactics that were initially used on Tehran.

Between November 2016 and January 2017, a variant of Shamoon re-emerged, and was used in attacks that deleted databases and files on dozens of public and private computer networks in Saudi Arabia. Among the entities struck was the General Authority of Civil Aviation, the Ministry of Labor, and the Saudi Central Bank. In the second wave of Shamoon attacks, files were overwritten with images of a 3- year old drowned Syrian refugee, hinting at the hackers' motivations.

2018 to Today

In March 2018, federal prosecutors unsealed indictments against nine Iranians accused of carrying out cyber attacks on behalf of the IRGC who stole data for financial gain from "144 American universities, 36 American companies and five American government agencies," as well as 176 universities across 21 foreign countries.

In **August 2018,** Facebook and Twitter purged hundreds of Iran-based groups and accounts that appeared to be part of a coordinated, inauthentic effort linked to Iranian state media to spread political content on four different continents, including in the United States. The unusual activity was detected by a private cybersecurity firm called FireEye, which alerted the social media companies. In a statement, FireEye said, "This operation is leveraging a network of inauthentic news sites and clusters of associated accounts across multiple social media platforms to promote political narratives in line with Iranian interests." The inauthentic pages sought to back Iranian foreign policy imperatives, and featured content that was pro-Iranian and pro-Palestinian, or anti-American, anti-Israeli, and anti-Saudi. Many pages reportedly promoted Quds Day, the Iranian regime-sponsored global day of protest against Israel.

In **July 2018,** Germany's domestic intelligence service found that Iranian cyber attacks targeting "the German government, dissidents, human rights organizations, research centers and the aerospace, defense and petrochemical industries" have been growing since 2014. The efficacy of the Iranian cyber attacks on Germany led the report's authors to conclude that the operations are initiated and guided by intelligence agencies.

In 2019, Iran engaged in a campaign of stepped up malign activities around the region as the Trump administration's "maximum pressure" campaign increasingly took effect, harming Iran's economy. As part of its campaign, Iran also stepped up its malign cyber activities. In June 2019, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) warned, "CISA is aware of a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies. … Iranian regime actors and proxies are increasingly using destructive 'wiper' attacks, looking to do much more than just steal data and money. These efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing."

In **July 2019,** U.S. Cyber Command tweeted that they discovered active misuse of a bug in Microsoft Outlook. FireEye traced the activity to a threat group called APT33, which is allegedly working at the behest of the Iranian government as part of a coordinated campaign against "U.S. federal government agencies and financial, retail, media, and education sectors."

In **November 2019,** a Microsoft researcher presented findings that the Iranian hacking group APT 33, the group behind the 2012 Shamoon attacks on Saudi Aramco, has undergone a dangerous evolution and shifted focus, moving away from attacks targeting IT networks in favor of efforts to infiltrate industrial control systems used in electric utilities, manufacturing, oil refineries, and related critical infrastructure. The researcher found that over the course of a year, APT 33 had launched crude password-spraying attacks at tens of thousands of targets, but in recent months, had narrowed focus to 2000 organizations per month while increasing the amount of accounts targeted at each organization ten-fold. The effort indicates that the group is seeking a foothold that would enable it to launch disruptive physical attacks at a time of its choosing.

In **December 2019**, IBM researchers announced they had discovered a new form of malware, dubbed "ZeroCleare," that is believed to have been created by Iranian hacking collective APT 34, a group with ties to the government. The malware was reportedly used in data deletion attacks on unnamed Middle Eastern energy and industrial companies in the preceding months. On December 29, 2019, the day the U.S. struck Iran-backed militia targets in Iraq in retaliation for earlier rocket attacks, Saudi cybersecurity officials detected a rapid effort to deploy a cyber attack using malware it nicknamed "Dustman." The target of the attack was subsequently revealed to be Bapco, Bahrain's state petroleum organization. The malware was highly similar to the "ZeroCleare" malware discovered earlier in the month, leading experts to conclude that Tehran was the likely culprit.

Following the January 2020 drone strike that killed IRGC Quds Force commander Qassem Soleimani, Iran-based attempts to hack U.S. federal, state and local government websites jumped 50% and nearly tripled worldwide. In February 2020, Reuters and Certfa exposed an Iranian hacking attempt—through Charming Kitten—targeting Israeli academics and researchers who study Iran. Hackers posed as prominent journalists who cover Iran, and asked for email credentials to preview interview questions all in an attempt to penetrate their targets' accounts.

As the world has struggled to respond to the COVID-19 pandemic, Iran has been one of the hardest-hit nations, driven in large part to various missteps taken by the regime. Despite facing an unprecedented public health crisis, Iran has continued its malign cyber activities unabated. At a press conference on March 20, 2020, Secretary of State Pompeo asserted that Russia, China, and Iran are carrying out online disinformation campaigns to stoke fear and discord in the U.S. On April 2, Reuters reported that hackers working in the interest of the Iranian government have since early March used advanced phishing techniques to try and steal the email passwords of staff members at the World Health Organization, presumably to gain access to intelligence that would aid in the fight against the coronavirus. Analysts believe the hackers were tied to Tehran as the malicious websites used to deceive the staffers were previously used in a campaign targeting American academics with connections to Iran. Similar incidents were reported, where Iranian hackers allegedly targeted British universities researching coronavirus vaccines as well as U.S. pharmaceutical company Gilead Sciences Inc.

In April 2020, suspected Iranian actors undertook an unprecedented campaign of cyber terrorism, attacking industrial control systems with the aim of injuring or killing Israeli civilians. Israeli media reported that six Israeli water facilities were targeted by Iranian hackers, causing irregularities in the operations of infrastructure and control systems at wastewater treatment plants, pumping stations, and sewage facilities that were detected in time to prevent a catastrophic outcome. According to Israeli and western intelligence officials, the most severe attack involved Iranian-written code, routed through American and European servers to disguise its origin, being used to hack into the software systems that controlled the water pumps at a major Israeli water pumping station with the intent of increasing the chlorine levels of treated water that would make its way to Israeli homes. The sophisticated attack was ultimately thwarted, but if successful, it could have sickened hundreds of civilians or triggered fail-safe mechanisms that would have shut off water for residential and agricultural use during a heatwave for those who receive water from the affected facility.

The attacks highlighted the vulnerabilities facing internet-accessible industrial control systems, and Israel's Water Authority subsequently ordered all facilities under its jurisdiction to update passwords to their control systems, reduce internet exposure, and ensure that all software is up-to-date. In particular, security researchers have found internet accessible human-machine interfaces to be a potentially vulnerable source of great risk at oil and gas, water, and power facilities. While major facilities tend to be well-protected, researchers have found that human-machine interfaces at some smaller and medium size facilities were susceptible to hacking. Once a malicious cyber actor gained remote access, they would be able to adjust critical inputs controlled by human operators, such as disabling alarms; starting, stopping, slowing down, or speeding up the operation of oil wells or gas pumps; or adjusting chemical levels in the water.

The head of Israel's National Cyber Directorate warned after the April attacks that "cyber winter is coming and coming even faster than I suspected," expressing concern that cyber attacks targeting civilian opulations would become increasingly commonplace now that Iran had breached a clear red line. For its part, the Iranian government denied culpability for the attacks on Israel's water system, claiming that Iran's cyber posture is purely defensive and that Iran could ill afford the blowback that would arise from trying to poison Israeli civilians. Iran's official protestations showed how Iranian officials seek to make use of the degree of plausible deniability offered by the cyber realm. As noted earlier in this report, if the attacks were in fact the handiwork of an ostensibly "independent" Iranian hacker collective, major attacks by such groups are typically bankrolled and coordinated by the IRGC, so the regime bears ultimate

responsibility.

The suspected Iranian cyber attacks on Israeli civilian water infrastructure touched off a cycle of tit-for-tat cyber attacks and reprisals between the two nations. In May 2020, Israeli officials revealed that then-Israeli Defense Minister Naftali Bennett greenlit a cyber attack that caused delays at a major Iranian port for several days. The Israeli reprisal was intended as a "knock on the door" to remind Iran of Israel's cyber capabilities and deter future aggression and was calibrated to only cause economic damage rather than harming civilians.

During June and July 2020, Iran was beset by a series of unexplained explosions and fires at military facilities, missile production sites, petrochemical, and industrial complexes, and, most notably, the Natanz uranium enrichment nuclear facility. While the origins of these incidents remain officially undetermined and some may have indeed been accidental or due to natural causes, the volume of explosions and fires over a short period points to an Israeli campaign of deliberate sabotage to set back Iran's nuclear program and malign regional activities. Israeli security officials cautioned that while "not every event that happens in Iran is necessarily related to us," Israel is committed to preventing a nuclear armed Iran and, to that end, "we take actions that are better left unsaid."

At least some of the explosions are believed to be the result of Israeli cyber attacks. Iranian officials blamed the most serious incident, the explosion at Natanz, which reportedly set Iran's nuclear program back at least a year, on a cyber attack, although other regional officials and an IRGC member who had been briefed told the New York Times that the explosion was caused by a powerful bomb that was smuggled into the facility. In response to the military threats against its nuclear program, Iran has begun reconstituting the damaged building at Natanz underground "in the heart of the mountains," according to the head of Iran's Atomic Energy Organization. Iran's hardening of the physical defenses of its nuclear program means that its adversaries will likely increasingly turn to cyber operations to try and set back Iran's nuclear progress.

In June 2020, hackers again targeted Israeli water management facilities, attacking agricultural water pumps in the upper Galilee and central Israel. According to the Israeli Water Authority, "These were specific, small drainage installations in the agriculture sector that were immediately and independently repaired by the locals, causing no harm or any real-world effects." While the attacks were not officially attributed to Iran, the similar nature of the attacks to the April 2020 attacks against Israel's water infrastructure points to Iranian involvement.

In October 2020, Israeli cyber security firms Clear Sky and Profero reported that they had identified a campaign of ransomware attacks targeting prominent Israeli companies and organizations the previous month by a hacker collective called MuddyWater (sometimes also referred to as TEMP.Zagros, Static Kitten, or Seedworm). According to Microsoft researchers, MuddyWater "is believed to be a contractor for the Iranian government working under orders from the Islamic Revolutionary Guard Corps, Iran's primary intelligence and military service." The MuddyWater campaign involved exploiting vulnerabilities in the Windows operating system that the affected organizations had not patched yet, allowing hackers to effectively take over their internal networks. The hackers were then able to install malware -- reportedly a variant of Shamoon – that would encrypt the data on computers within the network, blocking users from accessing them. Typically, these attacks are known as ransomware, as hackers will demand payment to restore access to the network. In this instance, however, the hackers did not seek payment, indicating their motivation was primarily to disrupt the affected organizations by preventing them from regaining access to

their data. The prioritization of harming Israeli companies over monetary gain suggests that MuddyWater's motive was primarily ideological, buttressing the belief that its hacking is carried out at the directive of the Iranian regime. The campaign was ultimately thwarted due to intervention by Israel's National Cyber Directorate, Clear Sky, and Profero.

Shortly after the revelation of the MuddyWater campaign, Iran reported that the country's port authority and one other unnamed institution had been targeted by cyber attacks that caused significant disruption. State media blamed the attack on Iran's "sworn enemies."

Cybersecurity researchers then revealed in December 2020 that Iranian hackers had launched cyber attacks involving ransomware, hitting 80 Israeli firms in November and December of 2020. The Iranian operation, known as Pay2Key, appeared to have been the handiwork of a state-sponsored hacking collective known as Fox Kitten, the name given to collaborate between APT33 (Elfin, Magnallium, Holmium, and Refined Kitten) and APT34 (OilRig, Greenbug). The Pay2Key attacks targeted dozens of companies in Israel's insurance, logistics, and industrial sectors, encrypting data on computers and workstations to make them unusable. Pay2Key also claimed to have penetrated the Israeli Aerospace Industries.

Pay2Key would, in some instances, issue taunting messages to affected firms and threaten to expose their data unless the companies remitted payments in BitCoin. Even after payment, Pay2Key did not turn over decryption keys in several instances and went ahead with leaks of sensitive information. Clear Sky assessed that the campaign's motives were primarily ideological and designed to incite panic in Israel rather than financial and noted that the wave of attacks caused significant damage to several of the affected companies. These incidents highlight that the Iranian cyber threat adds additional layers of insecurity at a time of international crisis.

The tit-for-tat campaign of sabotage between Iran and Israel escalated further in April 2021, as Israel is believed to have been behind an apparent cyber attack that triggered an explosion that caused a major blackout at the Natanz enrichment complex. The attack reportedly destroyed the power system that runs the facility's centrifuges and may have set back Iran's enrichment at Natanz by nine months. The incident occurred shortly after Iran announced the installation of new advanced centrifuges at Natanz and after Iran has begun enriching uranium to 60%, steps taken by Tehran to increase its leverage in negotiations with the Biden administration. At the time of the attack, Iran and the U.S. had just entered negotiations to restore compliance with the JCPOA, a development Israel opposes as it views the JCPOA as leaving Iran a pathway to a nuclear bomb. The attack underscored Israel's willingness to take matters into its own hands if it is dissatisfied with the direction of diplomatic efforts to resolve Iran's nuclear program. Iran has referred to the attack as "nuclear terrorism" and vowed reprisals, but Tehran is constrained by its desire to acquire sanctions relief. Its calculus may change, and it may even be compelled to target the U.S., which it views as complicit in Israel's cyberwarfare, if diplomacy breaks down.

Even during a critical point in the negotiations to revive the JCPOA, hackers linked to Iran's government attempted a cyberattack on Boston Children's Hospital in June 2021. In revealing the incident a year later, the FBI director called it "one of the most despicable cyberattacks I've ever seen." According to U.S. officials, the hack featured attackers exploiting Fortinet software to control the hospital's computer network. Earlier, in November, U.S. agencies warned that Iranian hackers had accessed "environmental control networks" at an unnamed children's hospital, which likely meant Boston Children's Hospital, which is one of the largest pediatric centers in the United States, and offers cancer treatment and heart

surgeries, among many other services. This shows that even in June 2021, when negotiators were reportedly making progress to revive the JCPOA—the actual negotiations themselves adjourned on June 20 for the Iranian presidential election—Iran's government was trying to attack critical infrastructure in the United States.

Beyond its escalating cyber warfare with Israel, Iran has also recently upped its cyber activities in terms of influence campaigns. U.S. authorities alleged that Tehran engaged in electoral interference during the 2020 U.S. presidential election by obtaining voter registration data and sending spoofed emails designed to intimidate voters and undermine confidence in U.S. democratic institutions. In December 2020, the FBI found that Iran had been behind a website called "Enemies of the People," which exploited claims of voter fraud in the United States to incite "lethal violence" against the FBI director, a former U.S. cybersecurity official, and state election officials who were involved in refuting the claims. The website posted these officials' home addresses and other personal information. These incidents demonstrate the growing investment Tehran is making in these kinds of operations, which target the United States.

Conclusions

The Iranian cyber threat poses unique challenges to American security given the difficulties with properly attributing attacks, the lack of clear-cut rules with regard to response options and concerns for escalatory responses, and the thousands of vulnerable sites throughout the country and among our allies and U.S. entities abroad that make for appealing targets. Iran has crossed a major red line by recently launching cyber attacks intended to cause harm to Israel's civilian populations by poisoning water systems and attempting an attack on Boston Children's Hospital. The main factor preventing Iran from launching major, disruptive cyber attacks against the U.S. homeland is not necessarily lack of opportunity or ability, but the regime's calculus as to whether the benefits of such an attack outweigh the costs it would likely incur.

To date, Iran has continually pushed the envelope in the offensive cyber realm, carrying out costly attacks against the United States and its European and Middle Eastern allies. Washington has mainly responded to increased Iranian regional provocations by engaging in its own cyber operations, for example, reportedly targeting an Iranian paramilitary database which enabled the regime to surveil and plan attacks against tankers passing through the Persian Gulf.

The levers at the U.S.'s disposal to mitigate the Iranian cyber threat are less than ideal. The U.S. has the authority under Executive Order 13694 to sanction entities engaging in malicious cyber-enabled conduct against the U.S., and is also able to issue indictments against Iranian cyber threat actors. But such actions are largely symbolic in effect.

This dynamic changed in September 2018, when President Trump issued National Security Presidential Memorandum 13 (NSPM 13), a classified directive that reportedly enables the White House to permit the military to engage in offensive cyber operations without a lengthy review process. The measure, which then-National Security Advisor John Bolton played an important role in crafting and implementing, is designed to deter adversaries from cyber campaigns targeting critical networks or interfering in U.S. elections. Bolton asserted that the directive would create "structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear." Cyber operations approved under NSPM 13 would have to fall short of the criteria for

classification as “use of force,” however, meaning they cannot cause death, destruction, or severe economic impacts. Still, the directive gives the Trump administration a potent tool to respond to and prevent Iranian cyber aggression.

Despite the issuance of NSPM 13, U.S. policymakers have yet to make full and concerted use of the authorities contained within. Iran has therefore yet to be deterred, as evidenced by reports that it has continued to probe critical U.S. systems, signaling that an attack on industrial control systems remains on the table. The primary deterrent to Iran undertaking the costliest and most destructive attacks would be the knowledge that such a cyber attack would lead to a kinetic response, but, troublingly, the U.S. has yet to define what constitutes an act of warfare in the cyber domain. Lawmakers of both parties have grappled with the question in the wake of the Soleimani assassination and have called on the Pentagon to provide guidance. Since 2011, it has been U.S. policy that, “When warranted the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.” Without clearly enumerated red lines, however, Iran is liable to test the waters in provocative ways, having already discovered it can carry out costly attacks on the U.S. financial system, on a casino, on universities, companies, and government agencies without significant pushback.

The most daunting task facing the U.S. is shoring up the defenses of the thousand soft targets around the country. The U.S. in 2018 elevated Cyber Command to a combatant command, and has made defending critical infrastructure against cyber attacks a key priority. Strategic collaboration with allied countries is an important component in ensuring that the U.S. and its allies are adopting best practices in cyber defense. In November 2019, the U.S. Cyber Command and its Israeli analog, the Israeli Defense Forces’ Cyber Defense Directorate, staged a joint exercise, dubbed “Cyber Dome,” in which the participants practiced responding to a simulated significant cyber attack. Israel has also opened its doors to other regional militaries to cooperatively share in its advanced cyber defenses. While such collaboration is useful for enhancing homeland security and protecting U.S. interests abroad, at the same time, the private sector in the U.S. has been largely left to its own devices when it comes to cybersecurity. A more proactive public-private approach is required to identify vulnerable targets and bolster cybersecurity across the board in order to achieve collective defense.