مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

Iran’s Cyberattacks Capabilities

January, 2020

Special Report

Iran's Cyberattacks Capabilities

Special Report

Table of Contents

Executive Summary

1. Iran is a master of asymmetric military capability, making use of terrorist proxies and lower-cost military technology to counterbalance the more technologically advanced forces of its foes. Successful international sanctions have limited Iran's ability to buy or develop high-end technology in almost every sector. However, a basic cyber capability—to conduct attacks or espionage against adversaries—can be obtained for the most part through accessing the Internet and educating oneself. Like a conventional weapon of war, a cyber capability can also be honed over time and improved through observing its impact on a target. This paper demonstrates that Iran has not only developed a range of cyber capabilities but is using them on a large scale to spy, attack, and steal.

2. Iran has been subject to damaging cyberattacks in the past, which have taught it the value of having its own cyber capability. In 2010, Stuxnet, a malicious covert software program spread throughout Iran's nuclear enrichment plant at Natanz, damaging equipment needed for the nuclear program. In 2012, a piece of malware called Flame was detected on Iranian computer networks, where it was covertly extracting and erasing data. Iran also used "cyber repression" to squelch online protests during the 2009 rise of the "Green Movement" by limiting Internet access and censoring or defacing Web content posted by protesters.

3. Nation-states usually empower an intelligence agency to run their cyber programs directly. By contrast, Iran's cyber workforce is a complex network of contractors, using private Iranian companies and internal academic institutions to undertake assignments from middlemen. These "cyber managers" proceed according to requirements and targets set by the Iranian Ministry of Intelligence and Security (MOIS) or the Islamic Revolutionary Guard Corps (IRGC). These contractor groups are not homogenous, and their efforts are sometimes combined for attacks, which makes it challenging to identify and track the exact perpetrators.

4. Iran uses cyberattacks for conducting espionage, accessing data, stealing intellectual property and spreading propaganda. Such state-sponsored cyberattacks are usually categorized as Advanced Persistent Threats (APT), although the majority of Iranian attacks are neither advanced nor persistent. Iranian cyberattacks typically use of a mix of approaches requiring minimal skills (e.g., phishing) combined with more sophisticated techniques to covertly access a target's network. This results in many attacks that are seemingly scattershot and amateurish, raising the prospect of detection by the target. Equally true, however, is the fact that with each attack that is detected, there is an increasing probability that the target will improve its defenses. However, Iranian cyber actors are caught frequently, with a small number even becoming publicly named and subject to indictment by the US government, yet the attacks continue and, simply by virtue of the large numbers, attacks do succeed with alarming frequency. Iran has managed to gain access to sensitive data on individuals through attacks on government and service sector targets. It has most likely stolen intellectual property from technology companies and accessed communication data from service providers.

5. Iran would like its own Stuxnet in order to attack and damage various industrial control systems (ICS) inside the petrochemical facilities that are so important to the economies of its adversaries. However, Iran has so far failed to develop such a capability and has instead focused on damaging the information technology (IT) networks of these targets. The Iranian capability to undertake such attacks, known as "Shamoon" is a data-wiping program that devastated IT systems in August 2012, November 2016, and December 2018.

6. Iran also makes effective use of open source research to engineer more targeted cyberattacks on individuals and to spread propaganda. However, in the future Iran will find its malicious use of social media will become increasing difficult thanks to new security initiatives by the platforms which have started to detect, block, and remove malicious accounts.

7. Iran continues to improve its cyberattack capability by developing both technical capability and innovations in targeting. Where traditional targets have become more aware of IT security, Iran now attacks weaker organizations in the supply chains of these targets, attacking on a global scale to obtain information or find “backdoors” through which to harm or steal from its primary targets. The majority of Iranian cyberattacks are on PCs, although Iran also has a basic ability to steal data from mobile devices. The latter is limited yet has already been seen to graduate to from solely domestic use in the past to international targeting. In addition, Iran will almost certainly continue the development and deployment of Shamoon. It is working to develop a means of ICS attack by stealing information from ICS suppliers in an effort to learn more about the vulnerabilities in such equipment. Iran may also be receiving assistance from Russia, supported by a public cyber bilateral memorandum of understanding and the detection of uncharacteristic Russian cyber activity in the Middle East.

1. Introduction

1.1. The goal of this paper is to draw together public research on cyber activity attributed to the Iranian state in order to draw conclusions about its current capability. There are a multitude of publications on Iran's cyber activity, and this paper does not seek to replicate nor enhance existing research, some of which has been undertaken by the world's top cybersecurity experts. Instead, this paper seeks to consider what this activity means from a strategic perspective and provide a summary of activity without requiring the reader to have a technical background. Where possible, the avoids extremely technical terminology, which is a pitfall for many papers written on any aspect of cyber technology.

1.2. Throughout this paper uses the term cyberattacks to refer an unauthorized penetration of a computer network or device by a third party. The initiation of an attack, or "hack" (a term used colloquially), is typically done through gaining user logon credentials, which is usually done through phishing, whereby the attacker entices a user to follow a link in an email from a seemingly reputable source. The link goes to a Web server under the attacker's control, which is used to either steal credentials with a reputable-looking but fake logon screen or by downloading malware (malicious software) onto the user's device. Spear phishing is the same process but with a better researched and enhanced interaction (e.g., an email impersonating an identified business associate of the target covering a familiar topic). Spear phishing requires greater target knowledge but also provides a higher chance of success. Spear-phishing attacks are carried out to steal information for intelligence purposes, gain further access, damage physical equipment, or spread propaganda. State-sponsored cyberattacks are usually categorized as APT, although in fact, many are neither advanced nor persistent.

2. Iranian Cyber

2.1. To begin, we must consider Iran's national security and foreign policy. Since the 1979 revolution, Iran has pursued an almost constant political collision course with other nation-states. Its government is a fusion of theocracy and guided democracy, which produces a security policy that is a cocktail of competing and overlapping factors: ideology of the Islamic revolution, perception of threats to the regime, long-standing national interests, and internal friction between political factions and institutions.[1] Iran seeks to enhance its international prestige yet has almost no true allies of significant international standing. Its political leadership has supported their nation's integration into international diplomacy, yet the supreme leader, Ayatollah Ali Khamenei, and key hardline institutions such as the IRGC oppose any change in the nation's security posture. It undertakes a veneer diplomacy while spending nearly a US $1 billion a year to support acts of terrorism,[2] which has made it the most active state sponsor of terrorism since the 1990s.

2.2. Iran is a master of asymmetric military capability, which is the result of successful international sanctions limiting its ability to either buy or develop military technology. Where it could not hope to compete with military aviation advances, it has instead concentrated on ballistic missile technology to reach its foes. Investment in an expensive and global blue water navy is on hold to enable it to build "swarms" of the small and agile fast attack craft. Instead of investment in conventional land forces, it has raised armies of terrorist proxies and paramilitary groups such as Hezbollah and the IRGC's Quds Force, which specializes in foreign missions, providing training, funding, and weapons to extremist groups and insurgents.[3] A cyber capability is therefore a logical and valuable extension to Iran's existing suit of asymmetric capabilities. In 2015 then–director of US national intelligence James Clapper testified before the US Congress that Iran "views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes"[4]

[1] Congressional Research Service, "Iran's Foreign and Defense Policies," October 8, 2019, https://fas.org/sgp/crs/mideast/R44017.pdf.

[2] "Countering Iran's Global Terrorism. Remarks by Nathan A. Sales, Acting Under-Secretary for Civilian Security, Democracy, and Human Rights," Washington Institute for Near East Policy, Counterterrorism Lecture Series, Washington, DC, November 13, 2018.

[3] The Counter Extremism Project, "The Islamic Revolutionary Guard Corps (IRGC)," 2019, https://www.counterextremism.com/threat/islamic-revolutionary-guard-corps-irgc.

[4] James R. Clapper, Director of National Intelligence, "Statement for the Record on Worldwide Cyber Threats," U.S. Congress, House Permanent Select Committee on Intelligence, September 10, 2015, https://www.dni.gov/files/documents/HPSCI%20 10%20Sept%20Cyber%20Hearing%20SFR.pdf

3. Origins of the Cyber Capability

3.1. Iran had an excellent teacher in the emerging art of cyber warfare; in 2010, Stuxnet,[5] a malicious and covert software program in the form of a worm, spread throughout Iran's nuclear enrichment plant at Natanz. The malware helped map the computer networks of the facility, including the connected ICS, and specifically targeted the programmable logic controllers (PLCs), control the electromechanical processes, in this instance causing fast-spinning centrifuges to tear themselves apart. It is believed that Stuxnet caused substantial damage and delays to Iran's nuclear program. The full Iranian response to Stuxnet is unknown but would have certainly led to significant costs and additional time to repair the damage inside the IT systems, many of which would require isolation for purging of the malware or perhaps would even need to be destroyed. Equally expensive industrial equipment would also have had to be replaced. Such equipment is only obtained by Iran through slow and covert proliferation networks. Moreover, there was also b the expensive hunt for the source of the program: determining how and by whom it was delivered into the facility.

3.2. In 2012 cybersecurity and antivirus firm Kaspersky identified a piece of malware on computer networks inside Iran that had the ability to covertly extract information from compromised devices including documents, social media conversations and keystrokes.[6] The malware, later named Flame, also had the ability to erase information. Flame is believed to have been active inside Iran since 2010.

3.3. Just prior to the attacks using Stuxnet and Flame, Iran experienced another lesson in cyberwarfare, this time while at war with its own people. A political movement arose in Iran after the 2009 Iranian presidential election, in which protesters demanded the removal of Mahmoud Ahmadinejad from office following what they viewed as a rigged outcome. This became known as the Green Movement, and the protests were aggressively challenged by Iran's security forces. However, Iran's young

[5] McAfee, "What Is Stuxnet?" https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware/what-is-stuxnet.html.

[6] Kim Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers," *Wired*, May 28, 2012, https://www.wired.com/2012/05/flame/.

population continued the protest through the use of Web content and social media, and in the process exposed this new, Internet-based battlefield as a key weakness in the Iranian state's ability to respond.[7] The government turned to the "cyber repression" of protests: limiting Internet access together with censoring or defacing the movement's Web content.

3.4. The Iranian regime needed to find personnel capable of undertaking this new sort of security activity, as it impossible to train the current federal employees with the skills needed to react effectively and on scale needed to meet the immediate issue. As a result, Iran turned to private individuals to undertake retaliatory cyber action, and several groups emerged under the control of IRGC and MOIS. Thus, Iran's new cyber capability was beginning to take shape.

4. Iranian Cyber Actors

4.1. Research from the Insikt Group concludes that following the rise of the Green Movement and the attacks by Stuxnet, Iran wanted to create a formal cyber organization but found itself unable to build a "politically and religiously reliable workforce."[8] Many of the qualified candidates for such an organization would be young, not favorable toward the government. and motivated more by financial gain than religious or political ideology. According to the Insikt Group, the answer was "tiered approach, with a network of people unofficially associated with the IRGC and Iranian government that were loyal to the regime and demonstrated sufficient religious commitment." This middle tier acted as the middlemen, translating, communicating, and assigning intelligence priorities into distinct cyber tasks, which were then bid out to multiple contractors. Insikt research found that "sometimes the contractors would compete with each other . . . [and] sometimes they would work together, but payment was only made once the objective was completed." The result

[7] Shannon Kandell, "Iranian Cyber Warfare: State Repression and International Retaliation," *Compass: The Gallatin Research Journal*, 2018, https://wp.nyu.edu/compass/2018/11/13/iranian-cyber-warfare-state-repression-and-international-retaliation/.

[8] Levi Gundert, Sanil Chohan, and Greg Lesnewich, "Iran's Hacker Hierarchy Exposed," *Recorded Future*, 2018, https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf.

was a sort of government-owned, contractor-operated (GOCO) arrangement that pits contractors against each other in their efforts to gain contracts and influence with the Iranian government.

4.2. The Insikt Group estimated that there are over fifty organizations vying for Iranian government-sponsored cyber projects. These projects are often compartmentalized such that two different contractors (or more) are typically required to complete the government-defined objective. These groups have been given a variety of colorful names by the cybersecurity research community, typically beginning with the word "Kitten" to signify Iranian origin, although where Iranian cyber actors are referenced in this paper, we have used one of the alternative naming conventions, which affords a more distinctive set of names for ease of recognition.

Cybersecurity companies such as FireEye[9] and Crowdstrike[10] have produced extensive reports on the activities and technical abilities of individual groups and continue to track their actions. The activities and assessment of these groups are a constantly changing picture, as much of the intelligence on these groups, outside of secret intelligence obtained by foreign states, is derived from their cyber activity rather than from the humans behind the keyboards. Notwithstanding, a handful of individuals have been named, mainly in US indictments, such as those working for the Mabna Institute, which was hired by the IRGC to break into the networks of hundreds of US universities, companies, and other victims to steal research, academic and proprietary data, and intellectual property.[11] We have their photos and basic physical descriptions thanks to the US FBI,[12] but we know little about their true motivations, affiliations, or careers.

[9] FireEye, "Iranian Reports," https://www.fireeye.com/search.html?q=iranian.

[10] Adam Meyers, "Meet the Advanced Persistent Threats: List of Cyber Threat Actors," February 24, 2019, https://www.crowdstrike.com/blog/meet-the-adversaries/.

[11] US Department of Justice, "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

[12] US FBI, "Iranian Mabna Hackers," https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers.

4.3. *Iran Threats*, a blog on cyber issues in Iran, offers the conclusion that "the ecosystem of Iranian actors is chaotic and ever changing, making disambiguating different campaigns and groups a troublesome process."[13] We can assume that individual Iranian contractors will move between companies; likewise, their software, code fragments, and attack infrastructure could be adopted by other contractors.

4.4. Iranian academic institutions may also serve as part of the toolkit available to the regime, either by enabling it to talent spot or working directly as part of the contractor cadre. Examples include Shahid Beheshti University, which has a specific cyber research institute, and the Imam Hossein University, which was founded by the IRGC and is subject to sanctions by the US government for supporting IRGC operations. In 2014 Ayatollah Ali Khamenei delivered an impassioned speech to Iran's university students, charging them prepare for cyber war.[14]

5. Capability

5.1. A review of cyber activity attributed to Iran in the past twelve months has been included in Annex A, which we will use to draw conclusions on capability. From this review it can be seen that a number of key Iranian groups were engaged in cyberattacks in 2019, including, as identified by the cybersecurity community, Elfin (A18, A17, A13, A4), MuddyWater (A8), OilRig (A12, A5), and Chafer (A16). Other groups are operational but have not yet been identified.

5.2. User credentials

5.2.1. The majority of *Iranian cyberattacks are initiated to obtain user credentials in order to gain access to computer networks*. Such credentials are usually obtained through *large-scale, unsophisticated phishing attacks*. However, Iranian groups

[13] *Iranthreats*, "Flying Kitten to Rocket Kitten, a Case of Ambiguity and Shared Code." December 5, 2017," https://iranthreats.github.io/resources/attribution-flying-rocket-kitten/.

[14] "Iran's Supreme Leader Tells Students to Prepare for Cyber War," *Russia Today*, February 13, 2014, https://www.rt.com/news/iran-israel-cyber-war-899/.

such as Elfin have conducted more sophisticated denial-of-service (DOS) attacks (A14)[15] and other groups have undertaken more developed spear-phishing efforts. The latter variety requires more advanced language skills and open source research; these groups are capable of both, although the use of high-volume, low-skill phishing efforts is the most popular method.

5.3. Stealing files

5.3.1. Once an Iranian cyber group has obtained access to a network or device, it has a *proven track record of being able to exfiltrate files covertly*. From the scale of the password-stealing attacks, it is evident that Iran is stealing data on a large scale against a range of targets.

5.3.2. This review's assessment of the typical information stolen by organization includes:

- Governments and the military
  - Espionage on political and military posture toward Iran, technologies, and information providing economic advantage
- Petrochemical suppliers
  - Information on facilities, plans, equipment, and staff
- Petrochemical equipment manufacturers and service companies
  - Technology; specifically, source code and equipment plans
- Telecommunications providers
  - Access to databases providing subscriber information, call or email records, and other telecommunications data such as geolocation information
- Travel
  - Access to databases providing travel manifests and client details to track targets

[15] The Domain Name System (DNS) is the system that translates a Web address into a physical Internet Protocol (IP) address. DNS attacks work by manipulating or hijacking the target organization's DNS in order to send users either to a different location or a circuitous route to said destination. The targets are lured to a destination or route under the control of the attacker (i.e., a compromised website containing malicious code).

- Individual dissidents
    - Obtaining information on dissidents’ movements and contacts
- Academic and science institutions and manufacturers
    - Intellectual property and technology

5.3.3. Targeting can be grouped into distinct areas: *stealing Internet Protocol (IP) addresses and information (government, manufacturers, academia, and dissidents), supporting wider intelligence access (telecommunications and travel), and seeking destruction (petrochemicals and government)*. This activity must generate significant data that will need translation from a range of languages combined with expert knowledge to exploit. One would predict that a large amount of information could be generated by the contracting out of Iran’s cyber workforce, whereby in some instances, success may equate with the volume of data stolen. This is especially problematic when the contractor lacks the expertise to evaluate what is stolen, a problem that is likely to occur, given the variety of targets. Iran could use its contractor workforce to evaluate stolen data, although the MOIS is also reported to have 30,000 officers, who could be put to work on this task.[16]

5.4. Destruction of data

5.4.1. Shamoon (A19) has set the global standard for the worst case in destructive attacks. Only the target, Saudi Aramco, the world’s richest company, could have survived such data and IT loss. *Shamoon has returned on three known occasions and will likely return again with an even higher degree of sophistication*. The success of Shamoon 1 may well be the product’s downfall, as it focused the cybersecurity community on developing the proper defenses and customers on buying them, and Saudi Aramco has not been successfully attacked again. Shamoon 2 and 3 have not been as successful as Shamoon

[16] US Defense Intelligence Agency, “Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance,” 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Iran_Military_Power_V13b_LR.pdf.

1, although improved target selection (e.g.. choosing a target that was less prepared) could produce a return to similar levels of destruction for subsequent versions. The Iranians are also taking care to select their Shamoon targets, covertly accessing the networks of targets for both versions 2 and 3 well in advance. Shamoon 3 also was intended to disrupt supply chains, which could be another way of hurting a principal target, such as Saudi Aramco, as it is now too difficult to attack such targets directly.

5.5. ICS

5.5.1. Shamoon caused widespread damage to the IT infrastructure of petrochemical companies, but it did not touch the ICS (the electromechanical systems and associated instruments used to control industrial processes). The attack methodology was probably developed to cause maximum damage in lieu of not having an ICS attack. *Iran is believed to be working on an ICS cyberattack but will find its development challenging*, as it will only have access to a subset of the equipment it needs to test due to sanctions preventing international sales. For example, even if Iran can discover the exact equipment installed inside a facility in Saudi Arabia, it will have limited knowledge and no access to test using the installed equipment.

5.5.2. Iran will have to steal this data from ICS suppliers. The Elfin group (A4) appear to have been tasked to obtain such information, although a complex system of resources and time will be required to reverse-engineer any stolen data. However, Iran is a determined protagonist and understands firsthand the damage a successful ICS attack could achieve. It will continue its efforts and may even seek such technology from a partner such as Russia (10.3).

6. Distributed Denial-of-Service Attacks

6.1. In computing, a distributed denial-of-service attack (DDoS)[17] is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

6.2. This review did not uncover any Iran-linked DDoS attacks during the period under review. This was traditionally a popular Iranian tactic: for example, a sustained DDoS attack was launched on US banks and other entities by Iran during the period 2011–2013.[18] DDoS protection services are now commonplace, and the absence of such attacks could be a sign that *Iran's targets are well protected against these types of attack.*

7. Mobile Devices

7.1. There is a *noticeable lack of attacks recorded against mobile devices* in the research as compared to the thousands of attacks against PCs. Iran's capability against mobile devices is to trick a target to download a fake messenger application (A9), which in turn can covertly extract data from the device. This is a limited approach as the fake apps cannot be planted in regular app marketplaces such as the Google Play store. The attack is also limited to Android devices as there is no way to install third-party applications on an Apple device. Notwithstanding, the Iranians have enjoyed some success with this approach and will continue to use and enhance this technique.

7.2. We can assume that Iranian cyber groups will be working to attack mobile devices directly (through their operating systems), but they *do not yet have this capability*. They also only have the capability to attack a device through a phishing attack, although successful penetrations of telecommunications providers may one day require another platform.

[17] Cloudflare, "What Is a DDOS Attack?" 2019, https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/.

[18] Eric Chabrow, "7 Iranians Indicted for DDoS Attacks against U.S. Banks," bankinfosecurity.com, March 24, 2016, https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989.

8. Social Media

8.1. Iran uses social media for distributing propaganda and to engineer spear-phishing attacks against individuals by masquerading as others (A16, A11). It has undertaken these activities for many years and with a degree of success, through publishing propaganda under an alias or using fake identities in order to gain connections with targets of interest. However, in 2019 such activities became significantly harder to achieve. Owing to the numerous scandals involving fake news, media outlets are more likely to check their sourcing and social media platforms now have increasingly robust registration and content checking. Facebook has proved to be particularly robust at removing networks of fake accounts spreading Iranian propaganda.[19] *We conclude that Iran will continue to use social media for propaganda but will find it increasingly hard to create fake accounts and maintain their activity, especially at a large scale.*

9. Signals Intelligence (SIGINT)

9.1. One of the possible reasons for Iran's large-scale approach to cyberattacks is that it *lacks a global SIGINT capability.*[20] This would be needed to allow Iran to collect communications data on its regional neighbors and global adversaries. Global SIGINT technology is only held by the world's wealthiest nations, such as the United States and its Five Eyes intelligence allies, Russia, and China. In addition, there are a small number of wealthy nations with limited regional capability who use military assets for data collection.

9.2. Years of near isolation for Iran have led to limited access to technology and training, limiting the ability to develop advanced technology. Iran also lacks overseas territories where it could deploy such technology to obtain an extended reach (e.g., Cuba for

[19] Facebook, "Removing More Coordinated Inauthentic Behavior from Iran and Russia," October 21, 2019, https://newsroom.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/.

[20] SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions. See US National Security Agency, https://www.nsa.gov/what-we-do/signals-intelligence/.

the Former Soviet Union). This may have led it to prioritize its offensive cyber efforts, and in particular, efforts to target telecommunications providers. *Penetrating these organizations will provide Iran with a significantly enhanced capability to identify and target individuals. This will improve its ability to mount spear-phishing attacks and even directly attack individuals through the provider's network.*

9.3. Nonetheless, Iran is developing a satellite collection facility, as reported by Jane's Intelligence Review in June 2018.[21] An analysis of the position of the site and its configuration by Jane's intelligence staff suggests that it is targeting communications satellites in synchronous orbits, including those of Israel, Saudi Arabia, and the United States. Iran also has the potential to access and intercept communications from a number of submarine cables that travel through its territory. Submarine cables are communications cables laid on the seabed between land-based stations to carry telecommunication signals across stretches of ocean. Such cables use optical fiber technology to carry digital data, which includes telephone, Internet, and private data traffic. There are cable landing stations at the Iranian cities of Bandar Abbas, Jask, and Chabahar.[22] One such cable, called Falcon, has connectivity to ten other nations, including Saudi Arabia.

9.4. *A SIGINT capability would significantly enhance Iran's ability to collect communications data,* as would the ability to access the traffic from submarine cable, which would add to its regional collection efforts. *This could make Iran less reliant on its traditional contractor-run cyber program against its neighbors*. However, it is equally true that *access to such data could augment the existing contractor-run capability by adding options for new data collection and infrastructure to attack its targets*. SIGINT technology is extremely expensive and requires advanced technology, so it will be difficult for Iran to implement any capability that would keep pace with its existing collection methods.

[21] Jane's Editorial Staff, "New Iranian Space Signals Facility Targets Satellite," June 2018, https://ihsmarkit.com/research-analysis/new-iranian-space-signals-facility-targets-satellites.html/.

[22] "Submarine Cable Map," TeleGreography, https://www.submarinecablemap.com/#/.

10. Foreign Assistance

10.1. Iran has no close and public alliances like the global friendships enjoyed by its neighbors, such as Saudi Arabia and the United States. Iran has a long-standing and complicated relationship with Russia, as, despite a mutual distrust, the two nations several political adversaries in common, including the United States, the United Kingdom, and the European Union. In 2012, the US Library of Congress reported on the intelligence relationship between Russia and Iran through cooperation between the Iranian MOIS and the Foreign Intelligence Service of the Russian Federation (SVR): Despite the two agencies' dissimilar doctrines and the complicated relationship between Iran and Russia in the past, they managed to cooperate in the 1990s, based not only on their intention of limiting US political clout in Central Asia but also on their mutual efforts to stifle prospective ethnic turbulence. The SVR trained not only hundreds of Iranian agents but also numerous Russian agents inside Iran to equip Iranian intelligence with signals equipment in their headquarters compound.(23)

10.2. There is a body of open source evidence to support a cyber relationship between Iran and Russia. As early as 2014, the US House of Representatives' Committee on Foreign Affairs heard testimony that a change in the national security balance between the United States and Iran involved a growth in "Iranian cyber capabilities and Iran developing a closer relationship with Russia." The statement explains that "in a very short period of time, Iran has moved from a Tier 2/Tier 3 capability to being almost world class in the cyber area, nipping at the heels of the United States, Russia, China, and Israel."(24) More recently, in March 2017, Iranian state broadcaster Press TV announced that Iran and Russia would be developing cybersecurity cooperation.(25)

(23) US Library of Congress, "Iran's Ministry of Intelligence and Security: A Profile, Report Prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the Combating Terrorism Technical Support Office's Irregular Warfare Support Program," December 2012, https://fas.org/irp/world/iran/mois-loc.pdf.

(24) "Iran's Support for Terrorism Worldwide, Statement of the Honorable Pete Hoekstra, Shillman Senior Fellow, The Investigative Project on Terrorism (Former Chairman of the U.S. House Permanent Select Committee on Intelligence)," US Congress, House, March 4, 2016, https://docs.house.gov/meetings/FA/FA13/20140304/101832/HHRG-113-FA13-Transcript-20140304.pdf.

(25) "Iran and Russia Announce Plans for Cyber Security Cooperation," Press TV via Youtube.com, March 15, 2017, https://www.youtube.com/watch?v=NaCukjiECWM.

It is not inconceivable that this would include cooperation on cyberattacks as well. Later in 2017, we may have seen the first fruits of this cooperation.

10.3. Triton: The Second Stuxnet

10.4. In December 2017, malware subsequently named Triton was detected in the safety systems of an unidentified petrochemical facility in Saudi Arabia.[26] The malware sought to reprogram industrial controllers used to identify safety issues. Fortunately, some of the targeted controllers entered a fail-safe mode, which caused related processes to shut down and the plant's engineers to identify the attack. Security company FireEye believes the attacker's actions inadvertently caused the shutdown while probing the system to learn how it worked.

10.5. Triton has subsequently been described as "*the world's most murderous malware* [emphasis added])*,*"[27] and it has been subject to extensive analysis by cybersecurity experts and by Schneider,[28] the manufacturer of the safety equipment. Triton gained access to the plant's network through an undisclosed attack, most likely via a phishing email or a USB device. It is critical that the *malware moved from the user network into the ICS equipment*, in this instance into a common type of controller user to manage industrial equipment. It is assessed that Triton's ultimate aim would have been to alter the safety limits within the controller and thus subsequently drive equipment into an unsafe state, which would not be acted upon. This, in turn, would cause a potentially catastrophic failure. Triton may have been used in a reconnaissance mode to learn about the system, perhaps to help Triton's development.

10.6. Iran was suspected to be responsible for Triton, given the location and type of target, although this would have marked a change in Iranian offensive cyber capability,

[26] Jim Finkle, "Hackers Halt Plant Operations in Watershed Cyber Attack," Reuters, December 14, 2017, https://uk.reuters.com/article/us-cyber-infrastructure-attack/hackers-halt-plant-operations-in-watershed-cyber-attack-idUKKBN1E8271.

[27] Martin Giles, "Triton Is the World's Most Murderous Malware, and It's Spreading, *MIT Technology Review*, March 5, 2019, https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/.

[28] "TRITON—Schneider Electric Analysis and Disclosure," January 23, 2018, https://www.youtube.com/watch?v=f09E75bWvkk.

which to date has not compromised any ICS equipment. Following further extensive analysis, FireEye determined that Triton was actually developed by the Russian government.[29]

10.7. Russia's choice to target Saudi Arabia for such a destructive attack was extremely unusual. The target could have been chosen as a remote test vehicle for Triton, but then why not choose another location in a less volatile region given the commonality of the equipment? Extensive research would have been required to identify the target facility; would Russia really conduct such research in an area outside of its traditional intelligence targets? These questions concerning the motive behind the attack suggest there was cooperation with Iran on at least the targeting of the facility. Iran does not have an ICS capability, but it has the strong desire and history to motivate it to conduct such an attack. Iran would have the access and intelligence to identify a suitable test target and would be assumed as the perpetrator if caught. Russia could have targeted this facility for a variety of reasons, including decreasing the risk of attribution of the test (if caught) while helping its Iranian cyber ally. We may never know the answer to this question, but we can be certain that *Russian assistance to the Iranian offensive cyber program will increase Iran's capability.* In October 2019 (A5), a Russian cyber actor was caught using Iranian cyber infrastructure to launch its own cyberattacks. The assumption was that Russia had hijacked the Iranians access, but could the two countries be working together?

11. Conclusion of Capability

11.1. Iran uses cyber as a core component of its asymmetric offensive capability (3). Cyberattacks are used for conducting espionage, accessing data, stealing intellectual property, and disseminating propaganda (5).

[29] "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," FireEye Intelligence, October 23, 2018, https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html/

11.2. Iran has been subject to damaging cyberattacks in the past, which have taught it the value of the capability and the possible use against its adversaries (3.1). Iran will continue the development and deployment of its Shamoon (5.6) malware to attach by erasing the computer's hard disk. Although cybersecurity developments and investments will harden targets against it. Iran has already started to switch its attacks to those on the supply chain of its principal target. An offensive ICS capability (5.7) is a clear priority, although technically difficult and expensive; Iran will doubtless seek to develop one through theft of information on these systems directly from their manufacturers. It may also be receiving assistance from Russia (10.3).

11.3. Iran uses cyber capabilities to meet its intelligence needs in lieu of access to a global SIGINT system (9), although it is developing such a capability. Attacks will continue against telecommunications and travel-related companies (5.5), with Iran seeking to gain access to databases providing intelligence on the contacts and movements of targeted individuals. These attacks will go increasingly global as new sources of data are discovered. It appears that Iran will seek a more advanced capability against mobile devices, as its current capability has severe limitations (7).

11.4. Iran has limited access to its adversaries and cannot send people to collect intelligence on the majority of its targets. As a result, cyber groups make effective use of open source research to identify targets and engineering convincing spear-phishing approaches. Social media (8) will continue to be used for approaching targets for spear phishing and spreading propaganda, even though the social media companies are making it increasingly harder for Iran to utilize their platforms, ultimately rendering the approach less effective.

11.5. Rather than develop an in-house government cyber capability, Iran has decided to make use of a network of contractors, using private Iranian companies and internal academic institutions (4). These groups are not homogeneous, and their efforts are sometimes combined for attacks. Their capability is mixed, with contrasting levels of skill seen between groups and even within an individual chain of attack. This makes the exact perpetrators of an attack challenging to identify and track. However, the international cybersecurity community generates an impressive amount of detailed reporting on these groups. This community will continue to develop an understanding as the Iranians develop their capability, although the internal management of these groups will always make exact and timely attribution difficult.

11.6. Iran makes use of a mix of low-skill attacks (e.g., phishing) combined with more sophisticated techniques to covertly access a target's network (5.4). This results in many attacks that are seemingly scattershot and amateurish. Such large-scale attacks have a high probability of detection, especially by technically capable targets. This approach could be due to a low capability of some cyber contractors or may be driven by the financial need to produce more quantitative results over a longer-term qualitative intelligence strategy. It is also unclear whether Iran has the capability to assess large volumes of information obtained from cyberattacks, especially if the attacks involve technical information. This could lead to a policy of engaging in more targeted collection, as we have seen with the group Elfin's attacks against ICS (A4), or a prioritization of more public and destructive intrusions.

11.7. Iran is a determined and aggressive player in cyber space. It attacks on a global scale with varying capability. Although it attempts to be covert in these activities, it gets caught on a regular basis. Iran does not appear to care that its efforts are revealed, as cyberattacks are used both for espionage and offensively as part of its approach to security.

12. Recommendations

12.1. Aside from ethics and political posture, military actions are deterred by the threat of greater retaliation. Cyber activity, which, like military action, is an intrusion into an adversary's territory, is not deterred in the same way. International policy on cyberattacks is still very much in development and should be the subject of further study; likewise, so should the psychology of the Iranian regime's view toward cyber and its "red line" for stopping an attack. These questions are too broad and academic for this paper, but we can examine factors that make it harder for the Iranians to execute successful cyberattacks.

12.2. Continued Investment in Cybersecurity Technology, Response, and Policy

12.2.1. Continued investment in cybersecurity is an obvious approach to mitigation. DDoS attacks are becoming less common thanks to new technologies, and phishing attacks are now more likely to be blocked by email security. Developments in the detection of artificial intelligence and the automation of responses have already limited the effectiveness of Shamoon, but they need to be developed continually as the Iranians will enhance their technology. Thus, continued and innovative investment is needed to keep pace.

12.2.2. Iran's cyberattacks tend to be targeted against multiple organizations simultaneously, which means that they are more likely to be detected. A successful defense strategy for one could also be used by all. As a result, Iran has achieved far fewer successful mass cyberattacks in nations with a coordinated cybersecurity framework.

12.2.3. Iran will not just attack obvious targets, and governments and large companies are not the only entities at risk. Iran has already begun targeting actors in the supply chain of its main targets and will seek new international targets if they hold data (telecommunications, travel or biographical) that it feels could add to its intelligence collection. As a result, the global awareness of the cyber threat posed by Iran should be increased.

12.3. Impede Its Cyber Workforce

12.3.1. Iran runs its cyber operations through contractors. Activities to deter these workers from undertaking such roles would impact their capability. The US government has charged numerous Iranian individuals with cyberattacks, but this has had no discernible impact on the pace of attacks. These individuals are unlikely to ever travel outside of Iran, so they must be aware they will not face US justice.

12.3.2. Iranian hackers will study their basic skills inside Iran but will have to conduct Internet research to keep up with the latest technologies. There may be creative ways to limit or frustrate Iranian access to such material online.

12.3.3. A destructive cyberattack against Iran's cyber contractors directly would be highly damaging to their capability. In 2019 there were public leaks of information on several Iranian cyber groups, including technical information and staffing. This must have had an impact on the morale of the groups as well as raised awareness of their attack methodology, which the cybersecurity community will now seek to mitigate. A sustained campaign of similar leaks may reduce the effectiveness of such groups to operate.

12.4. Limit the Effectiveness of Social Media

12.4.1. Governments should work with the major social media providers as well as those that are emerging to educate them on the dangers posed by Iran's cyber activities. It is in their interest to invest in processes to protect their users, given that the topic of inaccurate information and fake accounts is rarely out of the public eye. This will make it harder for Iran to exploit social media.

12.5. Internet Connectivity

12.5.1. If Iran continues to misuse its Internet connectivity to harm others, should the international community deny it access to the Internet? This is a radical and far-reaching proposal, but clearly a "disconnected" Iran would pose a far lower threat.

12.6. International Pressure to Stop Cooperation

12.6.1. Diplomatic pressure on the international community to prevent any cyber dialogue with Iran could prevent or at least slow the transfer of knowledge and technology from more advanced nations, such as Russia.

Annex A: Review of Iran Linked Cyberattacks

1. Cyberattacks are a newsworthy topic; research seeking to collate incidents leads to a deluge of results in reporting from media outlets, cybersecurity companies, private security researchers, and governments around the globe. This paper has reviewed the reporting of significant cyber incidents that have been attributed to Iran over a twelve-month period, including any connected incidents from before this period. This is in order to review recent capabilities which will be more relevant to whatever attacks might come in the future. This is by no means a comprehensive summary, as to do so would be near impossible; neither the detection of an attack nor its attribution to Iran can be done with 100 percent accuracy. Moreover, an unknown number of attacks fail to sufficiently penetrate their targets to warrant further investigation or may be misattributed to criminals or other nations-states, and thus are essentially lost in the "global noise" of malicious cyber activity. Finally, there are numerous groups operating within Iran, making the attribution of attacks difficult and sometimes inaccurate; this review has found that attribution changes with the passage of time.

2. The list of incidents has been sourced from a review of media reporting and information from the Washington, DC–based think tank, the Center for Strategic and International Studies (CSIS), which has published a timeline recording significant cyber incidents since 2006.[30] In addition the reporting and analysis of document leaks purported from Iranian cyber actors have been included; these have provided previously unknown details of targeting and attacks.

3. Reports are ordered by the date of publication, which is not necessarily the initial detection nor attribution of an attack, as some attacks (indicated where known) have been running for the course of months or even years before receiving publicity.

[30] CSIS, "Significant Cyber Incidents," https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

4. November 2019: Iranian Cyber Group Seeking an ICS Capability

4.1. Media reporting on a conference presentation by Microsoft assessed that an Iranian hacking group known as Elfin was seeking to develop an ICS attack capability.[31] Microsoft stated the group had traditionally targeted tens of thousands of organizations using a crude hacking technique of attempting to gain access to accounts using common passwords. ELFIN's approach has now narrowed to around two thousand organizations per month, while increasing the number of accounts targeted in each to almost tenfold. Microsoft ranked those targets by the number of accounts the group tried to crack, stating that "about half of the top 25 were manufacturers, suppliers, or maintainers of industrial control system equipment." Microsoft speculated that Elfin was seeking to develop a capability to conduct cyberattacks with physically disruptive effects against ICS.

4.2. **Assessment:** There would be little reason for Iran to seek to access the networks of ICS linked companies unless it was seeking to obtain information on such systems. Elfin has either refined its search to a smaller number of companies or has been told to concentrate its efforts in order to be more successful.

5. October 2019: Russian Actor Caught Using Iranian Infrastructure to Launch Cyberattacks

5.1. A UK-US government investigation revealed that an Iranian cyber operation had its activities compromised by Russia.[32] The Russian actor targeted covert command and control infrastructure set up by an Iranian hacking group known to researchers as OilRig (13). This infrastructure was setup by OilRig to launch its own attacks but was hijacked covertly by the Russian group to

[31] Andy Greenberg, "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems," Wired.com, November 22, 2019, https://www.wired.com/story/iran-apt33-industrial-control-systems/.

[32] UK National Cyber Security Centre, "Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims," October 21, 2019, https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims.

deploy its own covert software, which essentially rode on the shoulders of the existing attack. The Russian attacks were able to extract directory listings and files from the targets together with details of the Iranian activity. This included lists of active victims together with credentials for accessing their infrastructure. More than thirty-five countries were targeted, with the majority of the victims being in the Middle East.

5.2. **Assessment:** Not only has further Iranian cyber activity been exposed, but such activities have left systems vulnerable to others, increasing the potential for damage and data loss.

6. October 2019: Iranian Cyber Actors Caught Seeking Access to Email Accounts

6.1. From August to September 2019, Microsoft reported that a known Iranian hacker group had made more than 2,700 attempts to identify email accounts linked to specific Microsoft customers.(33) The group proceeded to attack 241 of these accounts. The accounts that were targeted were associated with a US presidential campaign, current and former US government officials, journalists covering global politics, and prominent Iranians living outside Iran.

6.2. Microsoft reported that the group gathered information from open source research and then used preliminary attacks to force a password reset or account recovery features in an attempt to take over the accounts. For example, the group would seek access to a secondary email account linked to a user's Microsoft account and then attempt to gain access to the primary account through verification sent to the secondary email. In some instances, the group gathered phone numbers belonging to their targets and used them to assist in authenticating password resets.

(33) Tom Burt, "Recent Cyberattacks Require Us All to Be Vigilant," Microsoft.com, October 4, 2019, https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/.

6.3. **Assessment:** Microsoft stated that the attacks "were not technically sophisticated" but noted that the attackers sought to use a significant amount of personal information both to identify the accounts belonging to their intended targets and to attempt the attacks.[34] We assess that the attackers made considerable use of open source information and must have dedicated significant amounts of time to gain access. The choice of targets is also interesting as it may show an interest in the US democratic process, something that has not been attributed to Iran before.

7. August 2019: Networks of Several Bahraini Government Agencies and Critical Infrastructure Providers Infiltrated by Hackers Linked to Iran

7.1. Various media outlets reported that computer networks were compromised belonging to Bahrain's National Security Agency, the Ministry of Interior and the First Deputy Prime Minister's Office.[35] There are no details of the nature of the compromise or any damage, although US media reported that US intelligence believed Iran was the likely culprit.

7.2. In July 2019, according to the same media reporting, the networks of Bahrain's Electricity and Water Authority were compromised, with "several systems shut down," and that "hackers were able to take limited control of several parts of the system." The same media report quoted unidentified "analysts and experts" who stated that the level of sophistication in these attacks was higher than in previous attacks attributed to Bahrain.[36] In addition, the Wall Street Journal reported that Aluminium Bahrain (Alba), one of the biggest smelters in the world, was also targeted, although the company subsequently issued a statement saying it had not been victim of a cyberattack.[37]

[34] Burt, "Recent Cyberattacks."

[35] Zak Doffman, "Iranian Hackers Suspected of Cyberattacks on Bahrain—A Warning beyond the Gulf: Report," *Forbes*, August 2019, https://www.forbes.com/sites/zakdoffman/2019/08/08/iranian-hackers-suspected-of-cyberattacks-on-bahrain-sending-message-beyond-the-gulf-report/#567af93a324b.

[36] Doffman, "Iranian Hackers."

[37] Bradley Hope, Warren P. Strobel, and Dustin Volz, "High-Level Cyber Intrusions Hit Bahrain amid Tensions with Iran," *Wall Street Journal*, August 7, 2019, https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488.

7.3. **Assessment:** The media reporting draws parallels with the Shamoon attacks (A19) in 2012.[38] These attacks caused widespread damage through wiping data from hard disks of affected systems but did not compromise ICS. Shamoon is undeniably attributed to Iran and has been seen twice. since in January 2017 and December 2018. As of the time of this writing, there is very little publicly available information on these new attacks.

8. June 2019: Leaks Detailing Unknown Individuals in Countries Surrounding Iran Targeted by Cyberattacks

8.1. An unattributed leak of data on messaging app Telegram provided technical information on an Iranian group known as MuddyWater, which was first identified in 2017.[39] This group was targeting individuals predominantly in Middle Eastern nations. However, it was also observed attacking other targets, including in India and the United States.

8.2. The Cybersecurity Company ClearSky published a detailed technical analysis of the leaked information, which targeted individuals using the same 2017 modus operandi: emailed documents masquerading as official correspondence but containing covert malicious code to gain the first stage of access to their device.[40] In this instance the documents claimed to be from government or major international actors (such as state telecommunications providers or the United Nations). The range of individuals targeted included the Iraqi, Tajikistani, and Pakistani governments; a communications company in Pakistan; unknown individuals in India, the United Arab Emirates and Cyprus; and Kurdish groups in Iraq.

[38] "Shamoon Virus Targets Energy Sector Infrastructure," BBC, August 17, 2012, https://www.bbc.co.uk/news/technology-19293797.

[39] Tom Lancaster, "Muddying the Water: Targeted Attacks in the Middle East," Palo Alto Networks, November 14, 2017, https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/.

[40] ClearSky Cyber Security, "Iranian APT group 'MuddyWater' Adds Exploits to Their Arsenal: Overview and Analysis of MuddyWater: New Infrastructures and TTPs," June 2019, https://www.clearskysec.com/wp-content/uploads/2019/06/Clearsky-Iranian-APT-group-%E2%80%98MuddyWater%E2%80%99-Adds-Exploits-to-Their-Arsenal.pdf.

8.3. **Assessment:** ClearSky reported that the attack used a known vulnerability and was rudimentary in its approach, which required the target to click through error messages, yet it was only detected by three antivirus engines. The fake documents are of high quality and relatively obscure, indicating that the attackers had conducted a significant amount of research into their targets using open source information. The choice of targets is broad and was presumably done for purposes of espionage. However, the inclusion of at least one telecommunications provider could indicate that one objective of the attacks is to enable access to further targets within these providers' networks. We do not know if these attacks were successful.

9. June 2019: Fake Mobile Applications Used for Espionage against Military Personnel in the Middle East

9.1. The cybersecurity company TrendMicro uncovered a range of fake Android mobile applications (apps) that masquerade as legitimate.[41] These apps mimic the appearance of messaging apps such as Telegram, Kik, or Plus but contain malicious functionality to exfiltrate data from their host device as well as covertly capture audio and video. TrendMicro monitored the command and control server used by the attackers and identified 660 mobile devices running the fake applications. Most of the affected devices were located in the Middle East, and much of the exfiltrated data was related to military matters, indicating that military personnel were targeted. The report references previous research by CheckPoint Research, which identified similar activity from 2016 to 2018 conducted against what were assumed to be largely Iranian domestic targets.[42]

[41] Ecular Xu and Grey Guo, "Mobile Cyber Espionage Campaign 'Bouncing Golf' Affects Middle East," Trend Labs, June 18, 2019, https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/.

[42] CheckPoint Research, "Domestic Kitten: An Iranian Surveillance Operation," September 7, 2018, https://research.checkpoint.com/ 2018/domestic-kitten-an-iranian-surveillance-operation/.

9.2. **Assessment:** Iran has the capability to attack and persist on mobile devices through the use of fake apps. These fake apps were not hosted by official marketplaces such as Google Play, and TrendMicro only observed the apps being promoted on social media. This indicates that targets of such attacks must have been directed to the downloads, either by spear-phishing emails or directly by malicious contacts (on behalf of Iran). The research also indicates a shift from using this technique domestically to international targets. This could perhaps be the result of increased Iranian confidence in the technique (from past success) as well as an ability to distribute and control the apps outside Iran.

10. May 2019: Leak of Objectives and Work of an Iranian Cyber Group

10.1. An unattributed leak of data on the messaging app Telegram provided copies of official Iranian government documents detailing "the Rana Institute."[43] The documents are labeled "secret" and appeared to have originated from MOIS. Analysis of the documents by ClearSky Cyber Security details Rana's objectives to track Iranians citizens outside Iran together with a slew of information on past cyber campaigns.[44] This includes details of attacks focused on hacking airlines to retrieve passenger manifests and hacking travel booking sites to retrieve reservations and credit card numbers. In some instances, specific but unnamed individuals are as referenced traveling on international flights. Additional targets include insurance, IT and telecommunications companies, as well as government agencies and departments on a global scale. It is not clear whether these attacks were only planned or had already taken place, and if the latter, whether they ended in success or failure.

[43] Catalin Cimpanu, "New Leaks of Iranian Cyber-Espionage Operations Hit Telegram and the Dark Web," Zero Day, May 9, 2019, https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/.

[44] ClearSky Cyber Security, "Overview and Analysis of Exposed Documents: Targets, Plans, and Attack Vectors," May 2019, https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf.

10.2. One document shows that the group were tasked by the IRGC to develop malware capable of damaging ICS but the “project was unsuccessful and did not achieve its goals despite a large budget.”[45] An additional document provides a screenshot of an attempt to conceal cryptocurrency procurement (perhaps due to the sanctions) using a virtualized environment (and by extension, appropriate connectivity) to masquerade as coming from India.

10.3. **Assessment:** The breadth of this leaked information is vast, especially as it implies original sourcing. The access to travel information is unusual, as it indicates the attackers are tasked with tracking movements of individuals outside Iran, presumably to correlate them with other, unspecified intelligence. The group’s objectives are reported to focus on Iranians, presumably those suspected of counterregime activities; however, not all the targeting is consistent with this, especially that of Israeli entities. This could indicate a targeting of Jewish ethnic Iranians residing in Israel or espionage against the Israeli government.

11. May 2019: Detection of a Network of Twitter Accounts and Fake News Stories Used to Spread False Information about the United States, Israel, and Saudi Arabia

11.1. Cybersecurity company FireEye[46] uncovered a large number of English language twitter accounts that were using fake American personas to espouse pro-Iranian views and negative content about Israel and Saudi Arabia. Some of these accounts impersonated real US citizens, including a handful of Republican political candidates. These fake accounts appropriated photographs and content from the candidates’ real accounts, making them difficult to distinguish from the latter.

[45] ClearSky Cyber Security, “Overview and Analysis.”

[46] Alice Revelli and Lee Foster, “Network of Social Media Accounts Impersonates U.S. Political Candidates, Leverages U.S. and Israeli Media in Support of Iranian Interests,” FireEye, May 28, 2019, https://www.fireeye.com/blog/threat-research/2019/05/social-media-network-impersonates-us-political-candidates-supports-iranian-interests.html.

11.2. In addition, a range of pro-Iran/anti–Saudi Arabia content was published in US and Israeli media outlets, with other accounts appearing to lobby journalists to cover specific topics. This enjoyed some success in prompting media outlets to interview US- and UK-based individuals on political issues. These deceptive approaches were published via the submission of letters, guest columns, and blog posts, mostly to small, local US news outlets. Many of these articles date from 201–2019, but some were dated as far back as 2015.

11.3. **Assessment:** This is evidence of a determined propaganda campaign, which must have taken significant time and good English language skills to orchestrate. This is not strictly a cyberattack but rather is included as an important cyber capability. The perpetrators must have spent significant resources researching target publications as well as managing the personas. FireEye's research notes that in one instance an account espoused views against Iran but then switched sides, perhaps in order to build an initial fan base from the US public. This shows a determined level of effort and sophistication in efforts to spread propaganda, with an additional impact of fueling distrust of media sources.

12. April 2019: Iranian Hackers Launch Attacks against Banks, Local Government Networks and Other Public Agencies in the United Kingdom

12.1. Various UK media outlets reported an update of a December 2018 attack that remains ongoing (as of April 2019) against the UK postal system and unnamed local UK government networks, officials, and banks.[47] In the postal system alone, personal details belonging to thousands of employees were stolen. There has been little official comment on these attacks although various cybersecurity experts have attributed it to Iran.

[47] "Iran Infiltrates UK Institutions in State Spying Attack," SC Media: The Cyber-Security Source, April 3, 2019, https://www.scmagazineuk.com/iran-infiltrates-uk-institutions-state-spying-attack/article/1581009.

12.2. **Assessment**: From the scant reporting available this would appear to be an attack to steal a vast number of credentials to allow for further deeper attacks on the target organizations. Furthermore, the attempts on UK officials would perhaps allow the attacker to subsequently impersonate them, which could provide even deeper official access or influence operations against the UK public. Although it is apparent the attackers enjoyed some success, an attack on this scale and breadth does make it easier to detect as it creates more "noise" as it targets multiple organizations, which are more likely to raise an alarm and coordinate a response. This will ultimately limit their effectiveness.

13. April 2019: Leak of Objectives and Work of an Iranian Cyber Group

13.1. An unattributed leak of data from the messaging app Telegram provided details of the tools, members, and victims of a known Iranian group called OilRig.[48] Cybersecurity researchers from the US security company Palo Alto Networks first identified the group in May 2016 and stated, "OILRIG is not particularly sophisticated, but is extremely persistent in the pursuit of their mission objective and, unlike some other espionage motivated adversaries, are much more willing to deviate from their existing attack methodologies and use novel techniques to accomplish their objectives."[49] In total, the leak contained details of 13,000 stolen credentials and further compromises of entities across 27 countries, 97 organizations, and 18 industries.

13.2. **Assessment:** The media reporting of the leak centers on compromises to Middle Eastern entities, both commercial and government, although the Palo Alto analysis shows that OilRig is targeting on a global scale. The group may well be operating on a global scale as well or seeking third-party access through suppliers and subsidiaries to its principal Middle Eastern targets.

[48] Ionut Ilascu, "Hacker Group Exposes Iranian APT Operations and Members," BleepingComputer.com, April 18, 2019, https://www.bleepingcomputer.com/news/security/hacker-group-exposes-iranian-apt-operations-and-members/.

[49] Bryan Lee and Robert Falcone, "Behind the Scenes with OilRig," Palo Alto Networks, April 30, 2019, https://unit42.paloaltonetworks.com/ behind-the-scenes-with-oilrig/.

14. March 2019: An Iranian Cyber Group Targeted Government and Industry Digital Infrastructure in Saudi Arabia and the United States

14.1. Cybersecurity experts report on the activities of an Iran linked group known as Elfin, which has been active since late 2015. Cybersecurity and antivirus company Symantec reported that the Elfin group specializes in scanning for websites containing known vulnerabilities. Once discovered, these sites are then attacked themselves or used as infrastructure from which to launch further attacks. The group has attacked at least fifty organizations, 42 percent of which were located inside Saudi Arabia and 34 percent of which were inside the United States. There was a broad range of targets, including governments, research organizations, and most commercial and industrial sectors. Symantec noted that 'some of these US organizations may have been targeted by ELFIN for the "purpose of mounting supply chain attacks. In one instance, a large US company was attacked in the same month that a Middle Eastern company it co-owns was also compromised."[50] These attacks consisted of spear-phishing emails. Symantec's research notes that Elfin's attack toolset is predominantly designed for espionage, as its techniques and tools are used mainly for gaining covert access to networks and devices to steal files. However, Elfin has also been linked to the destructive Shamoon malware (A19).

14.2. **Assessment:** Elfin is a determined attacker showing insight in using third parties in other countries to deliver supply chain attacks against its prime targets. The Symantec research reports a range of tools and techniques that the group has at its disposal, with constant revisions to update its approach as security improves. The group would appear to be tasked with espionage, although its "cyber reconnaissance" could be laying the groundwork for more destructive attacks if required.

[50] Symantec, "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S. Security Response Attack Investigation Team," March 27, 2019, https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage.

15. March 2019: Hacks of the Cell Phone of the Israeli Opposition Leader by Iran's Intelligence Service

15.1. Various regional media outlets reported that the leader of the opposition party in Israel, Benny Gantz, had his cell phone attacked by Iran, which stole personal and sensitive data.[51] The media support their claim by citing a supporting statement by Israel's internal security service (our research cannot locate this).

15.2. **Assessment:** This was just prior to the Israeli elections, and details of the attack were almost certainly overplayed for political gain. However. Gantz himself appeared to confirm the incident by claiming no sensitive data was stolen. Curiously. a second media report indicates that Russia was behind the attack, although it provides no supporting evidence.[52] This stands out as one of the few reports of Iran compromising a cellular device, but given the lack of detail and the unusual claim of Russian involvement, it is hard to assess its significance.

16. February 2019: US Indictment of a Former US Air Force Specialist Now Assisting in Iranian Cyberattacks

16.1. The US government charged several named Iranian nationals and former US Air Force counterintelligence specialist Monica Witt with cyberattacks and breaches of national security breach. Witt defected to Iran following a thirteen-year career in the US Air Force and as a military contractor; she was well placed to pass intelligence to the Iranian regime. However, it appears Witt also took on a more active role and worked with an unknown group of Iranian hackers to seek to compromise her former colleagues.[53] The group working with Witt created a fake Facebook account masquerading as a real

[51] "Israel Intelligence Agency Admits Iran Hacked Gantz's Phone," *Middle East Monitor*, March 16, 2019, https://www.middleeastmonitor.com/20190316-israel-intelligence-agency-admits-iran-hacked-gantzs-phone/.

[52] "Gantz's Phone Hacked by 'Russia' ahead of Israel Election." August 29, 2019, https://www.middleeastmonitor.com/20190829-gantzs-phone-hacked-by-russia-ahead-of-israel-election/.

[53] Thomas Claburn, "US Counterintelligence Agent Helped Iran Lob Cyber-Bombs at America, Say Uncle Sam's Lawyers," *Register*, February 14, 2019, https://www.theregister.co.uk/2019/02/14/counterintelligence_agent_espionage/.

US intelligence officer. Connections were then made from this account to other intelligence officers and then messages were sent to entice them to click on links to malware. The indictment makes no mention of whether the attackers managed to compromise any targeted systems, but the messages they sent were unsophisticated and amateurish.

16.2. **Assessment:** The defection of someone like Witt is a major coup for the Iranian government, and one can assume she gave them significant intelligence covering her career. It is apparent that Iran went beyond a simple debriefing and instead sought to use her in a more active role to assist with identification for direct targeting. However, this opportunity appears to have been wasted. given the amateurish approach to the final targets. This may perhaps show that Witt only passed names or confirmed photos on social media of the targets and was not involved in the execution of the attacks. Her target knowledge, if combined with US cultural knowledge and a fluent command of English, would have increased the likelihood of success.

17. January 2019: Security Researchers Identify a New Iranian Cyber Group

17.1. In early 2019 FireEye identified a new Iranian hacking group, now known as Chafer, which had been observed since November 2014.[54] Chafer prioritizes the targeting of the telecommunications sector, the travel industry and IT firms that support it, and the high-tech industry. FireEye concluded that Chafer's role is to track or monitor targets of interest to the Iranian state by collecting personal information, including travel itineraries, and by gathering customer data from telecommunications firms. Chafer uses the familiar vector of using phishing emails to steal user credentials from individuals or exploiting vulnerabilities in the Web servers of targeted organizations.

[54] Sarah Hawley, Ben Read, Cristiana Brafman-Kittner, Nalani Fraser, Andrew Thompson, Yuri Rozhansky, and Sanaz Yashar "APT39: An Iranian Cyber Espionage Group Focused on Personal Information," FireEye, January 29, 2019, https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html.

17.2. Kaspersky Labs published research covering the period of autumn 2018, when the majority of Chafer attacks during this period were actually inside Iran.[55] An undisclosed number of these targets were directed against foreign diplomatic entities inside Iran.

17.3. Assessment: Chafer would appear to have clear overlapping priorities with other Iranian actors, although it has diverged from these priorities in its internal targeting.

18. January 2019: Iranian Engagement in a Multiyear Global Domain Name System (DNS) Hijacking Campaign

18.1. FireEye reported that a group attributed to Iran,[56] which was subsequently identified in March 2019 as Elfin by Microsoft,[57] had targeted thousands of employees at more than 200 countries during the previous two years. The principal targets were oil and gas producers, heavy machinery manufacturers, telecommunications and Internet infrastructure providers, and governments in Saudi Arabia, Germany, India, the United Kingdom, and some parts of the United States.

18.2. The attack worked using a novel attack against the DNS, the system that translates a Web address into a physical IP address. The attack worked by manipulating or hijacking the target organization’s DNS in order to send users either to a different location or on a circuitous route to correct destination. Thus, the targets are lured to a destination or route under the control of the attacker. The wider system is then infiltrated and data are extracted. The attackers also managed to erase data on some of the machines they compromised.

[55] Denis Legezo, “Chafer Used Remexi malware to Spy on Iran-based Foreign Diplomatic Entities,” January 30, 2019, https://securelist.com/chafer-used-remexi-malware/89538/.

[56] Muks Hirani, Sarah Jones, and Ben Read, “Global DNS Hijacking Campaign: DNS Record Manipulation at Scale,” FireEye, January 10, 2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html.

[57] Chris Brook, “Iranian Hackers Stole Corporate Secrets; 200 Oil, Gas, Manufacturing Firms Targeted,” *Data Insider*, March 7, 2019, https://digitalguardian.com/blog/iranian-hackers-stole-corporate-secrets-200-oil-gas-manufacturing-firms-targeted.

18.3. Assessment: This was likely an extremely successful campaign of attacks to steal credentials and gain access to multiple types of targets. The attacks used tried and tested phishing of targeted individual, but owing to the more novel DNS attack, they did not require the complex social engineering of each target to convince them to visit the poisoned link. This was likely done for the purposes of espionage, to steal intellectual property, given the report of erasing data to cover up the access.

19. Shamoon: Malware Attacks in August 2012, November 2016, and December 2018

19.1. Shamoon 1

19.1.1. In 2012 one of the most destructive cyberattacks in history was launched against the petrochemical companies Saudi Aramco in Saudi Arabia[58] and RasGas in Qatar.[59] The attack, later named Shamoon after a word found in its code by security researchers, led to the destruction of 30,000 hard disks in Aramco and enormous disruption to operations, thanks to a near total loss of the company's IT network. Shamoon works by spreading within a network and writing corrupted data to the master boot record (MBR) of each hard disk it identifies: the MBR is the first readable area (sector) on a disk and identifies how and where an operating system is located so that it can be loaded (booted) into the computer's memory. [60] If the MBR is destroyed, the disk cannot be used and specialized forensic tools are needed to recover the remaining data. Finally, Shamoon reports back the IP address of each erased device to the attacker, perhaps to create a tally of its destruction. In this attack, the corrupted data contained the image of a burning American flag.

[58] Nicole Perlrothoct, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

[59] John Leyden, "Mystery virus Attack Blows Qatari Gas Giant Rasgas Offline," *Register*, August 30, 2012, https://www.theregister.co.uk/2012/08/30/rasgas_malware_outbreak/.

[60] Symantec Security Center, "W32.Disttrack.B," November 23, 2016, https://www.symantec.com/security-center/writeup/2016- 112300-5555-99.

19.1.2. The attack took place on both companies during the holy month of Ramadan, most likely as the attackers believed that many of the workers would be on leave. For Saudi Aramco it is believed that the attack first arrived into the network by an employee clicking a link in a spear-phishing email, but investigators still do not know when the email was sent or exactly what it contained.

19.1.3. Despite the destruction to corporate networks, the ICS systems were not attacked and production continued, although with significant disruption, as the administrative processes for maintaining and distributing production now had to function work without IT. The Cybersecurity website DarkReading.com interviewed Chris Kubecka, a consultant who worked on the security response inside Saudi Aramco, who stated that "Saudi Aramco had invested heavily in securing the ICS from cyberattacks, but the attackers crippled the company by targeting desktops, mail servers, and other Windows systems."[61] During the attacks a statement was released by a group calling itself "the Cutting Sword of Justice," which cited the reason for the attack as Saudi Aramco's support of the Al Saud royal family. The information security community agree that this group is an unknown Iranian actor.

19.2 Shamoon 2

19.2.1. In November 2016 cybersecurity company Symantec reported that Shamoon had been used once more, this time against multiple unnamed targets inside Saudi Arabia.[62] Symantec assessed that this version of Shamoon was "largely unchanged" from the previous version,

[61] Fahmida Y. Rashid, "Inside the Aftermath of the Saudi Aramco Breach," darkreading.com, August 8, 2015, https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676.

[62] Symantec Security Response, "Shamoon: Back from the dead and Destructive as Ever," November 30, 2016, https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever.

although this time, rather than an American flag, it used a photo of a body of Syrian child refugee who drowned in the Mediterranean in 2015. Similar to the first Shamoon attack, the attack was timed to occur after most staff had gone home for the Saudi weekend. There is also agreement from other cybersecurity companies that the perpetrators of the attack had sustained access to their target networks before launching Shamoon, using captured user credentials to broaden access.[63]

19.3. Shamoon 3

19.3.1. In December 2018 Shamoon was discovered again, initially in the networks of Italian petrochemical services company, Saipem, which reported that Shamoon "had wiped files from 300–400 servers and up to 100 PCs of a total of roughly 4,000 machines. The company said the attack mainly impacted servers in the Middle East, including Saudi Arabia, the United Arab Emirates and Kuwait, along with some devices in India and Scotland."[64] One of Saipem's customers is Saudi Aramco. Separately, Symantec reported that unnamed petrochemical organizations in Saudi Arabia and the United Arab Emirates had been attacked, although the extent of damage is unreported.[65]

19.3.2. In this latest iteration Shamoon was used once again to damage hard disks and used stolen user credentials to spread across networks. In this instance there is no reporting of an image being left behind. This version of Shamoon is also a more effective data eraser; the previous Shamoon damaged the MBR, rendering the drive unusable, but this version contained added functionality to erase files from the entire

[63] Robert Falcone, "Shamoon 2: Return of the Disttrack Wiper," Palo Alto Networks, November 30, 2016, https://unit42.paloaltonetworks.com/unit42-shamoon-2-delivering-disttrack/.

[64] Eduard Kovacs, "Shamoon 3 Attacks Targeted Several Sectors," *Security Week*, December 17, 2018, https://www.securityweek.com/shamoon-3-attacks-targeted-several-sectors.

[65] Security Response Attack Investigation Team, "Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail," December 14, 2018, https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail.

contents of the disk as well. While a disk attacked by Shamoon 1 could be unusable, files on the hard disk may still be forensically recoverable. However, if the files are first wiped by this new instance of Shamoon, recovery becomes impossible.

19.3.3. Assessment: Shamoon version 1 attacked two targets in the Middle East, version 2 attacked multiple targets in Saudi Arabia, and version 3 attacked targets in the Middle East and their suppliers in Europe, in what is perhaps a supply chain attack. All three versions required access to their targets' networks, which was most likely obtained from a low-skill phishing attack. However, security researchers note that once the malware is on the network, significant cyber reconnaissance is undertaken, perhaps by stealing more users credentials to allow greater access. Shamoon's targeting has grown more sophisticated, as has its ability to cause damage.

19.3.4. Unlike many attacks, Shamoon is not linked to a specific and named Iranian cyber actor. However, in the most recent attacks Symantec observed that one of the Shamoon targets in Saudi Arabia had recently been attacked by the Elfin group. They determined that there is a link between the proximity of these two attacks against this organization, perhaps with Elfin providing network access and reconnaissance for Shamoon. This does not necessarily mean that Elfin is behind Shamoon, as it could be that the group is working with another unknown group or indeed as part of a consortium of attacking groups.

King Faisal Center for Research and Islamic Studies (KFCRIS)

The KFCRIS is an independent non-governmental institution based in Riyadh, the Kingdom of Saudi Arabia. The Center was founded in 1403/1983 by the King Faisal Foundation (KFF) to preserve the legacy of the late King Faisal and to continue his mission of transmitting knowledge between the Kingdom and the world. The Center serves as a platform for research and Islamic Studies, bringing together researchers and research institutions from the Kingdom and across the world through conferences, workshops, and lectures, and through the production and publication of scholarly works, as well as the preservation of Islamic manuscripts.

The Center's Research Department is home to a group of established and promising researchers who endeavor to produce in-depth analyses in various fields, ranging from Security Studies, Political Economy, African Studies and Asian Studies. The Center also hosts the Library which preserves invaluable Islamic manuscripts, the Al-Faisal Museum for Arab Islamic Art, the Al-Faisal Institute for Human Resources Development, the Darat Al-Faisal, and the Al-Faisal Cultural Press, which issues the Al-Faisal magazine and other key intellectual periodicals. For more information, please visit the Center's website: www.kfcris.com/en

مركز الملك فيصل للبحوث والدراسات الإسلامية
King Faisal Center for Research and Islamic Studies

P.O. Box 51049 Riyadh 11543 **Kingdom of Saudi Arabia**
Tel: (+966 11) 4652255 Ext: 6892 Fax: (+966 11) 4659993
E-mail: research@kfcris.com