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

18

Dirasat

Rabi I, 1438 – December 2016

Deciphering Iran's Cyber Activities

Jack Caravelli & Sebastian Maier

Deciphering Iran's Cyber Activities

Jack Caravelli & Sebastian Maier

"The use of malware by state actors has altered the realities of cyber attack. History teaches that once weapons technology becomes feasible, states deploy it. Today the world may confront a dangerous technology race characterised by rapidly evolving and lethal weapons. Clausewitz believed that in warfare, the advantage rested with the defence. Cyber reverses that equation. It also offers the potential to build the fog of war through the ability to effect disruption, deception, confusion and surprise. We are only beginning to envisage the potential for different forms of malware, or the strategies or tactics employed to use it."[1]

(1) James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54:4 (2012): 114.

King Fahd National Library Cataloging-In-Publication Data

Caravelli, Jack
Deciphering Irans cyber activites. / Jack Caravelli; Sebastian Maier - Riyadh, 2017

32 p ; 16.5 x 23 cm

ISBN: 978-603-8206-19-5

1 - Iran - Foreign Relations 2 - Iran - National Security I - Sebastian Maier (co. author) II - Title

327.73055 dc 1438/5610

L.D. no. 1438/5610

ISBN: 978-603-8206-19-5

Table of Content

Abstract

This research paper explores the topical implications of the new realities and calculations surrounding Iran's rapidly-evolving cyber ecosystem. The study traces a variety of cases where attribution is overwhelmingly linked to cyber interference emerging from the Islamic Republic, in which perpetrators act at arm's length in an effort to insulate definitive accountability.

First, the findings include an in-depth account describing the strategic and technical ramifications of the infamous Stuxnet worm, a Western cyber attack that crippled nuclear centrifuges at the Iranian enrichment facility at Natanz in 2009.

Second, the paper outlines the lessons learned from Natanz, from an Iranian perspective, by shedding light on the country's increasing domestic efforts to centralize and professionalize its cyber clout. This is done in an attempt to streamline limited capacities, effectively making Iran a competitive top-tier player in the global cyber realm to date.

Lastly, the paper describes Iran's strategic departure in the aftermath of Stuxnet, moving away from mere defacement campaigns towards extensive cyber sabotage operations. Such a move resulted in repeated intrusive operations, either directly or through regional proxies, which hit the broader Middle East, the US and European nations from 2009 up until the present.

The Long Shadow of Stuxnet

Since at least the mid-1990s, the US government had been monitoring developments in Iran's nuclear program with growing alarm. Part of that concern centered on Iran's cooperation with a number of other nations in developing both its nuclear and missile programs. Those nations included Russia, China, North Korea and Pakistan. President Bill Clinton decided to take advantage of improved US-Russia relations after the breakup of the Soviet Union by contacting President Boris Yeltsin in an attempt to stop the flow of Russian scientific and technical support to Iran.

The result was the beginning of a diplomatic effort led by a senior US ambassador and a National Security Council official (Caravelli) to negotiate possible measures to mitigate the problem. Those measures were only partially successful and led to US sanctions against Russian entities known to be supporting Iran's programs.

After Clinton left office, Iran's programs continued to advance, raising alarms in Europe as well as parts of the Middle East. Direct negotiations with Iran began with the so-called EU-3—the British, French and Germans—who were later joined by the Americans in seeking to restrain threatening Iranian activities.

Those talks also did not advance very far, leading the United Nations Security Council to impose a series of resolutions that imposed a new set of sanctions on various Iranian entities and individuals. US sanctions remained in place and the Europeans added their own set of economic sanctions.

Despite those actions, by the time Barack Obama came into office the situation looked even more threatening than it did when diplomatic and economic sanctions began. The government of Israel was clamoring for possible use of military actions to stop Iran's nuclear and missile progress.

Obama came to office opposed to such drastic use of US military power. Like his predecessor, George W. Bush, Obama wanted to do something

less aggressive than military force but more aggressive than diplomacy and sanctions. This led to the decision to employ the first cyber attack against an Iranian target, the centrifuges which enrich uranium at Natanz.

In mid-July 2009, Wikileaks published a cryptic note stating that an Iranian informant had been arrested in connection with an incident at the Iranian nuclear enrichment facility at Natanz, which was reported to have occurred shortly before. The BBC announced at the same time that the head of the Iranian nuclear authority, Gholam Reza Aghazadeh, had resigned. Even then, there were speculations about ongoing clandestine activities in a counter-proliferation program framework, which Western intelligence services had been running against Iran for years.

What was later revealed and identified as the Stuxnet virus could have allegedly been part of what was at the time the largest covert manipulation of the electromagnetic spectrum: "Operation Olympic Games," of which Stuxnet was the malware of choice destined to infect Natanz, aimed at targeting critical infrastructure as diverse as power grids, public transportation and air defense systems.[2]

Such covert activities were likely established as an alternative if future Iranian-Western diplomacy over Iran's nuclear program was to fail, as well as to forestall "the military option" of an Israeli or US preemptive air strike.[3] The operational spectrum encompassed efforts to hinder and delay Iran's nuclear ambitions, including by means of targeted killings. For instance, Mostafa Ahmadi Roshan, an Iranian nuclear scientist who worked in the

---

(2) Another worm called "Duqu" was discovered in 2011. Unlike Stuxnet, to which it seems to be related, Duqu was designed to gather information rather than to interfere with industrial operations. In 2012, another spin-off, "Flame", was found purportedly used for operations of cyber espionage in the Middle East, and not exclusively in Iran.

(3) David E.Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *The New York Times*, February 16, 2016, accessed February 28, 2016, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?rref=collection%2Ftimestopic%2FStuxnet.

uranium enrichment plant at Natanz, fell victim to a magnetic car bomb blast in north Tehran in 2012.[4] In 2013, Mojtaba Ahmadi, reportedly one of Iran's leadinge figures in cyber defenses in his role as commander of Iran's Cyber War Headquarters at the time, was found dead in the north-west of Tehran.

The ramifications of the deployment of Stuxnet were considerable. Statistical data drawn from the International Atomic Energy Agency (IAEA) suggest that the number of actually operating enrichment centrifuges in Iran declined markedly as of spring 2009, despite the installation of more and more centrifuges. To that end, events in spring 2009 have likely limited the capacity of the Iranian enrichment program, possibly resulting in a delay of Iranian nuclear ambitions by approximately a year. As it turned out, the malware managed to cause centrifuge failure in a manner that would suggest flaws in design or material fatigue, rather than a deliberate act of cyber sabotage.

Acceleration centrifuges are complex, high precision tools that require exact control of vacuum, speed and gas flow. Thousands of centrifuges must be connected in order to achieve the necessary enrichment levels of the fissionable nuclear material. The analysis of Stuxnet now shows a fascinating detail: a part of the malicious software that intervened in the control processes seemed to have been distributed to many individual control computers to synchronize, and therefore amplify the damage output. Since every enrichment centrifuge of the many thousands was provided with a small, separate control computer device, the actually compromised parameters were deliberately put in sync, making it harder to detect them on the monitoring platforms.

Large-scale systems are now completely controlled by computers, rendering industrial complexes and plants vulnerable to targeted manipulation. Integral supply chains at industrial processes in refineries, chemical plants or nuclear power

(4) According to the Guardian, until 2012, the death of Roshan marked the fifth incident linked to targeted killing of Iranian scientists since 2010. https://www.theguardian.com/world/2012/jan/14/iran-accuses-us-britain-scientist Conversely, similar tactics have allegedly been used by Iran itself against opposing forces of the regime. Mohammed Hussein Tajik, purportedly former IRGC Quds Force commander of the "Iranian Cyber Army" was killed on grounds of accusations of spying and passing on security information to the "Green Movement" activists.

plants are nowadays operate, either partially or fully autonomously by computers in such a way that their temperatures, pressures and compositions are kept in a steady, controllable balance. The same accounts to monitoring software regulating cooling and inflow of new basic materials. Typically, industrial computer controls run based on Siemens' S-7 systems (SIMATIC automation tool), including automation tools as support for the adjusting and monitoring of sensors, such as electronic thermometers, control valves, engine speeds or cooling water pumps.

With such sensors at the very core of a variety of industrial security concepts, allowing mistakes such as deliberate manipulation to happen, serious disasters can potentially occur. The Stuxnet intrusion managed to deploy its destructive effect precisely because it aimed at being installed covertly as manipulation software into the heart of industrial controls, or SCADA (Supervisory Control and Data Acquisition).

Considering the enormous efforts that were spent on designing Stuxnet, the attribution of authorship to individuals, such as cyber criminals, can almost certainly be ruled out. In addition, the diligent purchase of the necessary intrusive components of such quality and reliability likely entailed high development costs that only state-owned or state-sponsored entities were able to allocate.

In many ways, Stuxnet ensured its distribution to be reliable and unnoticeable, as extensive investigations hinted that the virus could deploy its manipulative action only on a specific type of platform: the suitable Siemens-featured industrial plant. On all other systems - despite the infection with the same Trojan horse - nothing happened. Considered broadly, it goes to show that the architects of the attack must have had precise information about the structure of the system and the software used in it. Without an exact knowledge of the design and the manner of interaction between the individual S-7 components, an attack of this precision would not have been able to take place.

Therefore, only nation states may have been able to deploy the necessary resources, such as in intelligence gathering and conducting thorough testing on such a highly intrusive cyber weapon so as to make it virtually undetectable.

A closer examination of the small bits of indications and temporal correlations revealed circumstantial evidence about the inner architecture of Stuxnet. In September 2009, Symantec revealed that as close as sixty percent of infected machines were located in Iran. The worm was apparently programmed in a way that would have automatically stopped its spreading as of January 2009. Interestingly, computers on which the date was not set correctly – a seemingly irrelevant detail, yet oftentimes deliberately used to circumvent the expiry of time-bound software licenses – kept being affected until the worm was finally discovered. In the end, IT systems in over 150 countries were infected by the virus.[5]

The fact that Iran was using Siemens industrial control systems on a regular basis became well-known after export goods that were destined to some suppliers of the Iranian nuclear industry were accidentally intercepted. It became clear that the manipulation of such control systems could be used for catastrophic sabotage purposes. In March 2007, a team at the Idaho National Laboratory in the United States, launched a computer attack for test purposes and deliberately destroyed a power plant generator in its own laboratory.

A video of this attempt became public in September the same year, triggering a wave of panic in view of the vulnerability of the infrastructure in the West. It cannot be ruled out that the idea to sabotage the Iranian enrichment program through a sophisticated computer attack originated from the lessons learned at Idaho.

A question, however, remains: how did the attackers acquire the necessary know-how, including software access, to launch the attack?

An analysis of the considerable size and scope of the destruction that Stuxnet cause, most likely necessitated extremely nuanced information about the target infrastructure in question. It is conceivable that an Iranian defector brought the necessary data into the hands of the perpetrators. At the same time, it cannot

---

(5) Symantec provides an in-depth account detailing the technical nature of Stuxnet. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

be ruled out that the information was obtained in covert operations on the ground, which would fuel the assumption that the human factor in intelligence gathering still remains a critical part.

The unorthodox DNA that Stuxnet showcased in terms of how it spread only on specific system, suggests that the attacker had the means to physically plug in an infected USB device into the target system. At worst, the perpetrator was even able to steal blueprints and configuration details at Natanz: getting into the control system at Natanz could not have been done without the acquisition of precise data from the inner core of the Iranian plant to develop such a malicious code.

The aftermath of the attack shed light on an alarming insight: future criteria for assessing the safety of nuclear plants and systems could no longer be limited to the thickness of fortified concrete – the weak spot was the inner IT security infrastructure.

As such, it can be assumed that future cyber weapons will equally aim to hamper the ability of an adversary to synchronise and coordinate proper counter measures once the intrusion becomes apparent. Stuxnet masterfully succeeded in creating disorder and triggering the Iranians to distrust their own instruments. The idea was to mess with Iran's best scientific minds and make them feel as if they were incompetent at solving these issues.[6] Besides the technical repercussions, such as causing attrition upon resources and contributing to retarding the progress of the Iranian nuclear program, it is the psychological level that Stuxnet was targetint. Depriving operators of control, and causing a loss of belief in the operational ability to navigate such a crisis scenario, account to a clear strategic repertoire. The creators of Stuxnet merit recognition for making the most of this potential.

---

(6) James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54:4 (2012).

Centralization and Professionalization in Iran in the Post-Stuxnet Era

At the same time, the leaks from both the United States and Israel about Stuxnet being part of a wider, at the time largely unacknowledged offensive cyber disruption campaign, later dubbed "Operation Olympic Games," aimed at Iranian nuclear facilities, precipitated a wake-up call for the Iranians. Since then, Iran has expanded its cyber capabilities, cementing the country's now prevalent reputation as one of the top-tier cyber players globally.

The leaks provided Iran with an opportunity to attribute to its mortal enemies, the US and Israel, the cyber sabotage that its nuclear infrastructure suffered, recognize vulnerabilities, identify capacity gaps, and therefore learn the lessons by reverse engineering and generating similar algorithms for the purpose of launching its own attacks. Ultimately, Iran could embark on designing equally intrusive counterpunches with greater frequency and complexity, and, above all, execute them with far less stigma that could cause international outcry.

Iran has significantly professionalized its domestic technological cyber infrastructure, embodied by its infamous ambition to control, by means of segmentation, global internet data from domestic traffic. The Iranian regime has thus "evolved significantly in its exploitation of cyberspace as a tool of internal repression," just as much as it has demonstrated a "growing ability to hold Western targets at risk in cyberspace, amplifying a new dimension in asymmetric conflict."[7]

As with other countries where there exist limitations on free expression and restricted access to information, Iran has repeatedly resorted to extolling the alleged advantages of a centralized international communications transit to a limited set of gateways nationally. Such plans were presented and factually stated through the "Fifth Five Year Development Plan of the Islamic Republic of Iran", running from 2010-2015, mandating the formation of a "national information

(7) Ilan Berman, "The Iranian Cyber Threat, Revisited," (Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies), Washington, DC, March 20, 2013.

network" servicing e-government, as well as ensuring secure communications across sensitive governmental, military, corporate and ministerial bodies. Among other outcomes, this is a direct rejection of the original purpose of the internet which was to provide open and free access for all to share and exchange information. That approach is a direct challenge to all autocratic societies.

As a result, its parallel national web information network allows the regime to autonomously ensure critical network operations through deliberate segmentation of data traffic. Additionally, Iranian authorities are being enabled to failover internet sites from public to private networks, aggressively filter services through HTTP, and intercept traffic through either transparent or covert proxying, based on whether data stems from Iran or originates internationally.[8]

In the face of attacks such as Stuxnet, Tehran's push to promise domestic alternatives further facilitater the implementation of increasingly more comprehensive and restrictive measures on a national level. Amongst those are the total disruption of international connectivity, the prioritization of throughput, temporary throttling and bandwidth restrictions. Since the latter two options risk slowing down core components of modern-day business transactions and functionalities, these measures do continue to reflect concerns among parts of Iranian constituencies whether the Iranian government will utilize its grip on the internet for more widespread censorship than previously known.

After all, Iranian centralization of domestic peering through key points of control does not necessarily reduce dependency of its incoming physical internet infrastructure. Such dependency is critical to maintaining up- and downstream capacities. A clear demonstration occurred in October 2012, when the Kurdistan Workers Party allegedly induced an explosion of an outgoing pipeline carrying Iranian natural gas to Turkey. The kinetic damage did not just halt gas flow, but also severely disrupted Internet traffic connectivity to northern Iran and Iraq. The impacted fiber optics that were installed along

(8) Collin Anderson, "Dimming the Internet – Detecting Throttling as a Mechanism of Censorship in Iran, Iran Threats," *arXiv*, 18 June 2013. https://arxiv.org/pdf/1306.4361.pdf.

the oil and gas pipelines were provided by Turkcell Superonline, a Turkish internet and mobile services provider and cooperating with Telecommunication Company of Iran, TCI.

It appears that Iran's strategies of censorship have followed a historical trend of increasing precision of disruption when looking at it from a network-level granularity perspective. Whereas the June 2009 elections corresponded with a multiple-week outage of SMS services, by early spring 2013 keyword filtering on political slogans or terms associated with controversial issues had become a normal occurrence. In February 2012, the blocking of SSL – cryptographic protocols that provide communications security over computer networks - had shifted to the blocking of SSL of selected networks and the redirection of secure traffic through the interception of DNS requests that help locating and identifying computer services and devices connected to the internet.

By the same token, Iran's Internet users adopted more professional means to stem nascent censoring and interference by domestic intermediaries. The result is the deployment of sophisticated strategies by using anti-filtering tools to randomize or disguise network traffic in a way that makes intrusive, deep packet inspection increasingly costly Such mechanisms account, for instance, for the Tor and the Psiphon proxy tools.

There is general agreement that Iran goes to great lengths to streamline its cyber capacities not just at the strategic level, but also across its intervowen political and security apparatus. In 2012, Iran's Supreme Leader Ayatollah Ali Khamenei declared the creation of a Supreme Council on Cyberspace that included his representative responsible for the country's National Security Council, the speaker of the parliament, the commander of the Islamic Revolutionary Guards Corps, and heads of the judiciary and national police, as well as senior officials carrying responsible in the remits of information technology and science.[9]

---

(9) Barbara Slavin an Jason Healey, "Iran: How A Third Tier Cyber Power Can Still Threaten the United States," *Atlantic Council IssueBrief July 2013*, 4. http://www.atlanticcouncil.org/publications/issue-briefs/iran-how-a-third-tier-cyber-power-can-still-threaten-the-united-states.

The same year, Iran's armed forces announced the establishment of Cyber Headquarters that would work closely with the existing Cyber Council Committee along a variety of units – eg. politics, economics, and Islamic jurisprudence, to confront what Iran labels a soft-war campaign against Iran. [10] Moreover, thousands of cyber experts are said to be trained by the IRGC's own Cyber Defense command to spy on dissidents at home and surveil sizeable Persian diaspora communities such as in the US, Sweden or Germany.

Saudi Arabia in the Crosshairs – Shamoon, Shamoon 2

Since Iran ramped up and streamlined its cyber capabilities following the Stuxnet attack, it has been suspected of retaliatory attacks on a regional and global scale in a variety of cases.

Consider for instance the August 2012 attack aimed at the computer network of Saudi Arabia's state-owned oil giant, Saudi Aramco. The incident, most probably triggered by Iranian hackers, neither harmed hardware nor humans physically. Yet, the attack, called "Shamoon," managed to erase the hard drives of an estimated 30,000 computers. In a sign of lacking resilience and backup plan in the aftermath of the intrusion, the company reportedly had to resort to half a dozen computer security firms in order to prepare a forensic investigation. Saudi Aramco also had to send buyers to Asia to procure thousands of replacement hard drives.

While the attack likely failed to effectively disrupt and halt production output, it certainly caused considerable monetary damage, as well as immeasurable reputational damage. As part of the investigation findings, the attack involved spear phishing, fake emails trying to trick users into engagement that allows a hacker to secretly install malicious software in an effort to hi-jack computer systems. In doing so, Shamoon forced Aramco, the world's largest oil producer,

(10) Joanna Paraszczuk, "Iran Establishes Cyber HQ As Shadow War Continues," *JerusalemPost*, December 3, 2012, http://www.jpost.com/Iranian-Threat/News/Iran-establishes-cyber-HQ-as-shadow-war-continues.

to isolate an entire portion of its electronic systems from outside access, while the investigation could not confirm any signs of insider involvement by an Aramco employee.

A group calling itself "Cutting Sword of Justice" claimed responsibility for the attack, which, according to the Wall Street Journal was tied to Iran.[11] Their motives were in large part political, as the hacker group openly blamed Saudi Arabia for committing atrocities in nearby countries of Bahrain and Syria.

Merely two weeks after the Aramco incident, RasGas, at the time Qatar's second largest LNG producer and gas carrier, became the victim of another cyber sabotage. The malware attack was most likely affecting gas extraction and critical processing only rudimentarily, and yet, both incidents showcase the larger repercussions when companies are being targeted by cyber attacks. All modern economies rely heavily on uninterrupted supply of oil and gas, as well as reliable prices. An interruption of deliveries from Saudi Arabia and Qatar would greatly intensify global economic stress in the energy sector, likely translating into significant uncertainties on global stock markets.

In November 2016, and with increasing frequency as of late January 2017, Saudi authorities issued alerts advising vigilance in light of the resurfacing of variants of the Shamoon worm that crippled Saudi Aramco in 2012. Similar warnings have been disseminated, as the Saudi labour ministry and the hub of the local petrochemicals industry in the Saudi eastern Province experienced similar network disruptions. Another victim was the Sadara company, an American Saudi joint venture, as it was forced to shut down its computer networks, although the forced downtime allegedly had not affected the operational capabilities at its facilities in the industrial city of Jubail. Recent international commentaries on Shamoon 2 suggest that its design and intrusive architecture very much resembled its predecessor from 2012. Even extensive technical examination on the latest malware attack revealed

(11) Siobhan Gorman and Julian E.Barnes, "Iran Blamed for Cyberattacks," *The Wall Street Journal*, October 12, 2012, https://www.wsj.com/articles/SB10000872396390444657804578052931555576700.

striking similarities in terms of the Dos files that caused the wiping of disks across infected systems.[12] In many ways this is surprising, as hackers are normally expected to conceal their intrusive strategies by adding variants and enhancements - in conjunction with the principle of adaptability – and anticipation of bolder preventive countermeasures than experienced in 2012.

Interestingly, according to Dimitri Alperovitch, CTO at Crowdstrike security firm, one of the major features of Shamoon2 was to display on the affected desktops the highly sensitive imagery of the three-year-old Syrian boy who was washed up on a beach on Turkey in 2015. In 2012, Shamoon left an image of a burning American flag before crippling the computer platform.[13] Such symbolism is relevant as it underpins and highlights the ongoing tension between countries on both sides of the Arabic Gulf that exist in the broader geopolitical and strategic arenas across the region. Displaying offensive cyber capabilities appear to be increasingly important as part of translating robust national interests through non-linear and intrusive means of warfare in the cyber domain. From both an offensive and defensive viewpoint, such a reading is clearly in line with the growing significance of cyber to national security in the years to come.[14] Similarly, the importance of tightening regional coordination to stem cyber threats aimed against the entirety of GCC countries have been echoed by remarks by Saleh Almotairi, Director General of the newly established Saudi National Cyber Security Center, Ministry of Interior, during the recent 2nd Cyber Security Conference in Riyadh in late February 2017.[15]

---

(12) Greg Linares, "An analysis of the Shamoon2 malware attack," *Vectra Networks*, February 7, 2017 https://blog.vectranetworks.com/blog/an-analysis-of-the-shamoon-2-malware-attack.

(13) Dmitri Alperovitch, "Shamoon Round 2 or the Power of Machine Learning," *crowdstrike*, December 1, 2016, https://www.crowdstrike.com/blog/shamoon2/.

(14) Timothy Edmunds, Complexity, Strategy and the National Interest, International Affairs 90:3, 2014. 533,534.

(15) "IISS Cyber Report: 23 February to 2 March 2017" http://www.iiss.org/en/iiss%20voices/blogsections/iiss-voices-2017-adeb/march-8a0c/cyber-report-23-february-to-2-march-0217.

Disrupting the West: Operations Saffron Rose and Ababil

In 2013, three years after the initial revelations of the computer worm Stuxnet, a California-based cyber security company by the name of FireEye unveiled an extensive report about increased threat activities by the so-called Iranian "Ajax Security Team." References linked the hacker group to Iran by exposing an increase in attacks, code-named Saffron Rose, aimed against US American defense companies as well as Iranian dissidents living abroad. Nart Villeneuve, senior threat intelligence researcher at FireEye, asserted that these efforts were consistent with Iran's attempts to control political dissidents by means of expanding their offensive cyber capabilities. He contended, "Iran is not just quantitatively expanding its cyber activities, there is also a transition towards more sophisticated cyber espionage tactics, where hacks are no longer carried out simply to spread messages, but also to infiltrate systems and compromise them in the long-run."

"This group, which has its roots in popular Iranian hacker forums such as Ashiyane and Shabgard, has engaged in website defacements since 2010. However, by 2014 this group had transitioned to malware-based espionage, using a methodology consistent with other advanced persistent threats in this region." [16]

The Ajax Security Team also conducts its actions against domestic Iranian users of the anti-censorship technologies Proxifier and Psiphon, as both are able to bypass the internet censorship system in Iran. While it remains unclear whether Ajax Security is working in isolation or part of a larger, possibly state-controlled effort, it is safe to say that the team draws from malware tools that do not seem to be freely available to individuals such as criminal entrepreneurs. Instead, the group uses various social engineering tactics to lure targets and infect their systems with tailored malware, and likely possesses means and exploit codes to launch extensive zero days attacks.

---

(16) Pierluigi Paganini, "Ajax Security Team lead Iran-based hacking groups," *Security Affairs*, May 13, 2014 http://securityaffairs.co/wordpress/24923/cyber-crime/ajax-security-team-iran.html.

FireEye has also revealed information about more than 70 outgoing destinations of a suspected command-and-control server. All connections were discovered when analysis of malware samples showed signs of being disguised proxies of the aforementioned Iranian censorship circumvention tools. The examination revealed a suspicious pattern, as the majority of targets carried "Iran Standard Time" zone, and ran on Farsi. What is more, of the 33 connections that deliberately did not run on Iran Standard Time, one third was still set up as Farsi while the rest ran on compromised Proxifier and Psiphon installations.

This is one specific example that has, however, been paralleled by many others. Iran has already been identified with advanced cyber attacks since 2009, when plans of a U.S. Presidential Marine Corps helicopter suddenly surfaced on an Iranian file-sharing network.[17] One year later, the so-called "Iranian Cyber Army" halted Chinese search engine Baidu, in connection to the platform referring negatively to political messages emanating from Iran.

In 2013, the Wall Street Journal reported that Iranian actors had intensified their efforts to impede important US infrastructure facilities. Finally, in recent years, another group called Al-Qassam launched Operation Ababil, which caused a series of DDoS attacks – or distributed denial of service attacks - against major US financial institutions, including the New York Stock Exchange. Simultaneously, Al-Qassam introduced more advanced DDoS attacks by flooding banking websites with large volumes of encryption requests. Since these processes consume considerable system resources, for instance when dealing with encrypted online customer transactions, banks can face temporary server disruption or even collapse. Such traffic flooding operations hit major institutions including Wells Fargo, U.S. Bancorp, HSBC, JPMorgan Chase and CitiGroup.

Concurrently, in April and May 2013, US officials and corporate IT security experts were alarmed by a series of destructive cyber attacks that hit American

(17) Martti Lehto, *Cyber Security: Analytics, Technology and Automation*, ed. Pekka Neittaanmäki (Springer International Publishing: Switzerland), 2015, 74.

energy companies. These were potentially sent as probes for future attacks examining ways to take control of processing systems, like oil pipelines. After a month-long probe into the design and scope of destruction, the alleged source of the attack was narrowed down to emanating from Iran, precipitating a warning from the Department of Homeland Security. The apparent multipronged front that hit the US energy sector appeared sophisticated enough to assume the attacks being signed off by Iranian government authorities, although final evidence could not be brought to the fore.[18]

In the grand scheme of things, these hostilities shed light on Iran's determination and progress achieved in improving its offensive hacking skills. And yet, even though the logic of the attacks against the US energy and financial sectors show a similar pattern as the intrusions experienced at Saudi Aramco and Qatari RasGas the year before, "attributing political cyber attacks, if executed professionally and if unsupported by supplemental intelligence, is very hard if not impossible. Even if an attack can be traced to a particular state, and even if that state's motivation to attack seems clear, the attribution problem's technical, social, and political architecture gives the accused state sufficient deniability."[19]

The skill and sophistication needed to design and launch such cyber sabotage capabilities may indicate that these efforts are less driven by motivations associated to more traditional cybercrime since no bank accounts were breached or customers' assets taken. Rather, the existing grey areas that render definitive attribution so difficult are part of a deliberate strategy that may hint at military involvement under Iranian governmental guidance in retaliation for Western cyber attacks and the regime of economic sanctions set in place at the time. Or, in the words of Michael Hayden, former director of the CIA and the NSA, "I've grown to fear a nation state that would never go toe-to-toe with us

(18) Nicole Perlroth and David E.Sanger, "New Computer Attacks Traced to Iran, Officials Say," *The New York Times*, May 24, 2013. http://www.nytimes.com/2013/05/25/world/middleeast/new-computer-attacks-come-from-iran-officials-say.html.

(19) Thomas Rid, *Cyber War Will Not Take* Place (London: C Hurst & Co Publishers Ltd) 2013.

in conventional combat that now suddenly finds they can arrest our attention with cyber attacks."[20]

Cyber Proxy Activities in Syria, Yemen and Lebanon

In April 2013, the so-called "Syrian Electronic Army," an unofficial group of hackers who support the Assad-regime, and likely maintain ties to Iranian counterparts, managed to hijack the Twitter account of Associated Press and sent a fake tweet reporting an alleged explosion at the White House. Unsurprisingly, the tweet erased the equivalent of $130 billion in equity market value, and sent the New York Stock Exchange plummeting.[21]

The group has also carried out devastating cyber-attacks against the Syrian opposition since the onset of the Syrian Civil war as early as 2011, often using the anonymity of online platforms to its advantage. The SEA's steep learning curve in using cyberspace more proficiently for its use hints at the involvement of Iranian advisors in training at the tactical lower levels of command structures, in keeping with the de-facto presence of Iranian intelligence advisors that oversee military action of pro-Assad regime forces in Syria. The SEA's cyber espionage campaign towards the end of 2013 hit a number of high-ranking figures within the Syrian opposition, such as former chief of staff of the Supreme Military Council (SMC), Salim Idris, a defected former Syrian Army general, who was in charge of the command structure of the armed wing of the Free Syrian Army at the time.

In spring and summer 2015, a group called the Yemen Cyber army (YCA) arose, and claimed having successfully penetrated into Saudi Arabian governmental

---

(20) "Cyber experts warn Iranian hackers becoming more aggressive," *Reuters Summit News*, May13,2014. http://www.reuters.com/article/us-cyber-summit-iran-hackers-idUSBREA4C03O20140513.

(21) Max Fisher, "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?" *The Washington Post*, April 23,2013. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.cae0913d3cae.

systems, including the Interior, Defense and Foreign ministries. According to statements of Saudi-owned London-based newspaper Al-Hayat, their IT infrastructure has also been subject to attempts of the pro-Houthi YCA that displayed anti-West and anti-Saudi slogans in Arabic, presumably indicating Iranian interference in the cyber campaign.

It is noticeable that the YCA attacks showcased at times the tagline "Cutting Sword of Justice," a slogan that was used in the Saudi Aramco attack in 2012, and appears seldom elsewhere on the Web. In addition, YCA's activities were corroborated as exclusive cover stories by Fars News and NewsQuickLeak.ir, communication footprints in Iran. The YCA, like the Al-Qassam cyber brigade, and the Iranian Cyber Army, maintain a comparatively low profile in its propaganda activities on social media channels, a rather odd characteristic if they were considered to act autonomously without overarching strategic guidance.

Looking to Lebanon, a country long associated with being prone to political divisions stretching over more than a generation, it is hardly surprising that Iran's major Lebanese ally there, Hezbollah, has upped its ante in cyber, too. A March 2015 report by CheckPoint, an Israeli provider for IT security, sheds light on the granularities and functioning of a cyber attack operation it called Volatile Cedar, suggesting evidence that lead to the suspicion of the threat originating from Lebanon, and possibly being supported by Iran.[22] The malware, labeled Explosive, targeted multinationals and the defense sectors around the globe since 2012.

Connecting the Dots of Iran's Global Cyber Outreach

In summer 2015, cyber intelligence provider ClearSky issued an equally-detailed report about an even more intrusive deployment of malware, code-

(22) "Volatile Cedar: Threat Intelligence and Research Report," *CheckPoint Software Technologies Ltd.*, March 30, 2015. https://www.checkpoint.com/downloads/volatile-cedar-technical-report.pdf.

named Gholee; in over 500 occasions the malware penetrated targets, almost 50 percent of which occurred in Saudi Arabia, and 14 percent in Israel. A variety of characteristics of the malware included the use of native Farsi, indications of interface language changes to Farsi, and tracing back of IP addresses to locations in Iran.[23]

It is no coincidence that ClearSky's discovery of Gholee shares by and large the same characteristics as the malware found by US-based IT company FireEye in regards to the "Ajax Security Team." Forensic investigations vis-à-vis cyber interference in other places in the Middle East and Europe are very much in keeping with the narrative of threat actors being located in Iran.

In March 2015, the Japanese security company TrendMicro detected cyber attacks similar to the patterns of Gholee in both Germany and Israel – presumably initiated by a hacker group funded by the Iranian government. The cyber attack was given the name "Woolen Goldfish" by Trend Micro. The attack is described technically as a relatively simple, yet extremely effective maneuver for espionage and phishing of data. As part of the investigation, attribution was linked to the Iranian hacking community "Rocket Kitten," whereby it is assumed that Mehdi Mahdavi, under the alias "Wool3n.H4t," developed the attack itself based on a software variant that previously existed in 2011, modifying it further to operational exploitation.

"Woolen-Goldfish" was based on tailored phishing e-mails destined to supposedly high-ranking recipients; the messages contain a link that leads potential victims to a file in a free online storage service. This file – disguised as a PowerPoint document – infects the target system in the background with malicious software (e.g. spyware trojan, keylogger). The keylogger then logs all the user's tactile inputs on the target system and passes them on to the attacker. The exact technical sequence is described in detail on the homepage of Trend Micro.

---

(23) Thamar Reservoir, "An Iranian cyber attack campaign against targets in the Middle East," *ClearSky Cyber Security*, June 3, 2015. http://www.clearskysec.com/thamar-reservoir/.

As mentioned above, the attack method itself was neither new nor exceptionally sophisticated. However, this does not detract from the success that manifested itself as demonstrated by the large number of infiltrated targets. In addition to Iran, the People's Republic of China and the Russian Federation have also been found regularly practicing "spear phishing" attacks for years, having all of the earmarks of an advanced persistent threat (APT).

In the case of "Woolen-Goldfish," as in many other cases, the malware was hidden in a simple e-mail. Messages of this kind are adapted with formal standards to which any targeted recipient might be accustomed, presenting the user with no obvious reason not to click on the infected file attachment or link. Such attacks are generally preceded by a methodically-sophisticated approach called "social engineering." It refers to interpersonal manipulation with the aim of inducing certain behaviors – luring, for example, into the divulgence of confidential information, the purchase of a product, or the release of funds. "Social engineers" spy out the personal environment of their victims, deceive identities, or use certain behaviors such as authority to obtain secret information or unpaid services.

In November 2014, German state Bavaria's internal intelligence agency revealed that Iranian hacker attacks targeted numerous Germany-based research institutions and international companies in other EU countries, US, Israel, Mexico and China. According to the reports, significant amounts of data were stolen, including sensitive material regarding the manufacturing of military and civilian technology, including rockets, helicopters, satellites and unmanned aerial devices. The investigators encountered a server on which the purported attackers saved captured files of victims as well as tools, leading to the revelations of the perpetrators' working hours and IP addresses, hinting that the tracking ended in Iran.

The German government's existing cyber security capabilities are designed to protect businesses and institutions from fraudulent activity and industrial espionage. However, currently they do not match up for the security sector's

ambition and daring willingness to name the origin of the threats, let alone work towards appropriate means to counter cyber threats originating from places such as Iran. The bottom line is that attribution, at the very least from a European perspective, has as much to do with political will as it does with technological and infrastructural capability.

Conclusion

In contrast, the vertical target distribution presented in the various cases above correspond and align with the topically-reigning geopolitical climate and nation-state interests, hinting at the the motivation to achieve goals in cyber espionage and sabotage, rather than monetary gain or some sort of hacktivism. It can therefore reasonably be expected that Iran's political ascendance and assertiveness carries an increasingly prominent cyber outlet as an extension of its ongoing proxy-campaigns across the region.

There also is a broader element. We conclude that Iran's cyber activities are designed and intended to advance Iran's geo-strategic goals not only in the region but in countering not only Israeli or friendly Arab nation cyber defenses but also those of the United States. Beyond the problems caused by the Stuxnet virus, Iran has paid a very low price for its aggressive cyber offensives. As demonstrated by Russia and China, much chaos and disruption can be achieved against an enemy through cyber attacks and at very low risk.

There is very little likelihood that the international community through the United Nations Security Council, for example, would devise an approach that mitigates what "cyber aggressive" nations such as Iran would do in the future. As such, those who oppose Iran in the Middle East and beyond almost certainly will have to contend with a theocratic regime set on disrupting the international order.

About the Authors

Jack Caravelli is the previous principal adviser of President Bill Clinton on Russia and Middle East nonproliferation issues. His extensive career in government service includes analytic, staff and managerial positions at the Central Intelligence Agency, the White House National Security Council staff and the Department of Energy where Caravelli directed the department's international nuclear threat reduction programs. Since leaving government service, he has authored four books and speaks on various national security issues in the US and abroad. In 2015 he chaired an international cyber conference in Lugano, Switzerland and is chairing another international cyber conference at Oxford later in 2017. He also has written on cyber issues, including for the UK publication "Cyber Security Review." Caravelli appears regularly on national television and radio programs. In 2016 he became chair of NewGen Global, an international technology advisory company.

Sebastian Maier is a Resident Research Fellow at King Faisal Center for Research and Islamic Studies since 2015, where he focused on politico-military trends in the Middle East, Syrian conflict, and the involvement of Russia, Iran, and Hezbollah in the Levant. Prior to his work at the Center, Maier worked as a trainee at the Canadian embassy to Germany, as well as the German-Saudi Liaison Office for Economic Affairs in Riyadh. Maier received a Bachelor's degree in Political Science and Law in 2013 from the University of Munich and SciencesPo Paris and earned his Master's degree in Intelligence and International Security from the Department of War Studies in 2014 at King's College London. Since 2016 he provides strategic advisory services to governments and international corporations.

King Faisal Center for Research and Islamic Studies (KFCRIS)

King Faisal Center for Research and Islamic Studies is an independent non-governmental institution founded in 1403/1983 in Riyadh, Saudi Arabia. As envisioned by the late King Faisal bin Abdulaziz, the Center seeks to be a platform for researchers and institutions to preserve, publish, and produce scholastic work, to enrich cultural and intellectual life in Saudi Arabia, and to facilitate collaborations across geopolitical borders. The Chairman of KFCRIS board is HRH Prince Turki Al-Faisal bin Abdulaziz, and its Secretary General is Dr. Saud bin Saleh Al-Sarhan.

The Center provides in-depth analysis on contemporary political issues, Saudi studies, North African and Arab Maghreb studies, Iranian studies, Asian studies, Modernity studies, Energy studies, and Arabic language studies. The Center also organizes conferences, collaborates with prestigious research centers around the world, employs a group of distinguished researchers, and maintains contacts with a wide range of independent experts in different disciplines. The Center is home to a library containing rare manuscripts, an Islamic art museum, King Faisal Memorial Hall, and a visiting fellows program. The Center aims to expand the scope of existing literature and research so as to bring to the forefront of scholarly discussions the contributions and roles of Muslim societies in the humanities, the social sciences, literature, and arts–historically, as well as today.

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: 8692 Fax: (+966 11) 4577611
E-mail: research@kfcris.com