Iran's Activity in Cyberspace: Identifying Patterns and Understanding the Strategy

Gabi Siboni, Léa Abramski, and Gal Sapir

This essay presents the evolving Iranian cyber activities with the purpose of identifying patterns that presumably form the cyber strategy applied by the regime to external and internal threats. The paper initially describes Iranian cyber operations, based on information released by the Islamic Republic and reports published by cybersecurity firms. The work then follows with an analysis of Iranian cyber activities. The article draws the characteristics and dynamics of Iran's cyber activities, both externally and internally, defensively and offensively. This survey highlights four common patterns identified in the research on Iranian cyber activities and is followed by an analysis of the main findings.

Keywords: Iran, cybersecurity, national cyber strategy, force buildup, internal and external threats, offensive and defensive activity

Introduction

Over the past decade, international observers may have minimized Iran's cyber capabilities as the relevant information documenting their existence is limited; however, perceptions of the Iranian threat have recently changed. At the 2019's edition of Cyber Week in Israel, Yigal Unna, the director-general of the Israel National Cyber Directorate affirmed that Iranians are among the five most active state actors in cyberspace. He stated that "the Iranians have

Prof. Gabi Siboni is the head of the Cyber Security program at INSS. Léa Abramski is a research intern at INSS. Gal Sapir is a research assistant in the Cyber Security Program at INSS.

been continuously active for a long time deploying broad attacks, including attacks to gather intelligence, influence operations, as well as attacks intended to cause harm and destruction to systems. Iran is one of the only countries to execute destructive attacks."[1] This recent shift in the way the Iranian threat is perceived among Western countries raises questions about the growing level of Iran's capabilities. It might be particularly noteworthy to identify the Iranian threat and to outline the characteristics of what appears to be Iran's national cyber strategy led against its adversaries. Indeed, experts have observed an intensification of Iranian activities in cyberspace, which is well documented by cybersecurity firms. According to a Microsoft survey published in March 2019, Iranian cyber groups have targeted thousands of people and more than 200 companies around the world during the past two years, causing significant damages estimated at hundreds of millions of dollars.[2]

Since the early twenty-first century, Iran has invested a significant portion of its budget in improving cyber capabilities. In the first three years of President Rouhani's first term (2013–2017), the security budget increased by 1,200 percent.[3] Frank Cillufo, director of the Center for Cyber and Homeland Security and the vice president of George Washington University, declared in 2017 that "in recent years, Iran has invested heavily in building out their computer network attack and exploit capabilities. Iran's cyber budget had jumped twelvefold under President Rouhani, making it a top-five cyber-power. They are also integrating cyber operations into their military strategy and doctrine."[4]

Two major events were pivotal in the development of Iranian activities in cyberspace. The first is the internal civilian protest that took place in 2009, known as the "Green Movement" and coined the "Twitter Revolution" by

1 "The Israel National Cyber Directorate: Iran Is a Main Cyber Threat on the Middle East," *Israel National Cyber Directorate*, June 26, 2019, https://www.gov.il/en/departments/news/unna_cyber_week_2019.

2 Robert McMillan, "Iranian Hackers Have Hit Hundreds of Companies in Past Two Years," *Wall Street Journal*, March 6, 2019, https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036.

3 Ben Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018, https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

4 Sam Cohen, "Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests," *Cyber, Intelligence, and Security* 3, no. 1 (2019): 71–94.

foreign media outlets. In the wake of the Iranian presidential election of 2009 and the disclosure of Ahmadinejad's victory over his main opponent Mousavi, massive protests took place across Iran to challenge the election's results.[5] Claiming that the election was rigged, the protestors wore green, the color of Mousavi's campaign, which gave name to the protest movement. Despite the regime's repression, the protestors were active for many months after the election. They concentrated their efforts on utilizing social media channels, such as Twitter, Facebook, and YouTube, for organizational purposes and as a platform to convey updates and information both inside and outside of the country. This remarkable use of information and communication technologies (ICT) helped to strengthen the movement while the government struggled to thwart its activity. This situation forced the Iranian regime to improve its understanding of cyberspace and its proficiencies to operate in this field. The development of a cyber strategy became a vital necessity.

The second major event—the attack known as "Stuxnet"—is considered decisive in the pursuit of a national plan to build Iran's cyber capabilities. The Stuxnet malware was discovered in 2010 and targeted Iranian computer systems.[6] The exact activity of Stuxnet remains unclear, suggesting a longer operating period from its conception to its disclosure.[7] It caused the self-destruction of almost a thousand centrifuges—around a fifth of all active centrifuges at the Natanz's nuclear enrichment facility, significantly delaying the Iranian nuclear program.[8] The impact of this malware exposed the vulnerability that states have experienced with the increased interconnectedness of most of the critical sectors. The emergence of new technologies also emphasized the need for enhanced security needs to protect and defend states in cyberspace.

In addition, economic pressure and the impediment of the nuclear program fostered social and economic resilience. The Iranian utility to turn to resilience seems to be by using "hybrid tools," including cyber activities. To this end, the development of cyber capabilities should be seen in many

5 "Editorial: Iran's Twitter Revolution," *Washington Times*, June 16, 2009, https://www.Washingtontimes.Com/News/2009/Jun/16/Irans-Twitter-Revolution/.

6 Josh Fruhlinger, "What Is Stuxnet, Who Created It and How Does It Work?," *CSO*, August 22, 2017, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

7 "The Israel National Cyber Directorate: Iran is a Main Cyber Threat on the Middle East."

8 Taylor Armerding, "Whatever Happened to Stuxnet," *Synopsy*, January 17, 2019, https://www.synopsys.com/blogs/software-security/whatever-happened-to-stuxnet/.

ways as a means of the Islamic regime for competing against its internal and external adversaries.

The following section will examine facts, events, figures, and official statements in order to identify common patterns and comprehend Iranian cyber activity. These characteristics will then enable analysis and understanding of Iran's presumed cyber strategy.

Confronting External Adversaries

Over the years, the Iranian regime has set up a cyber array that includes organized hacker groups operating under its various security organizations and independent groups operating in the interest of the regime. In addition, several groups and states in the Middle East receive Iranian support and function effectively as envoys operating on behalf of Iran's cyber interests. This aim of this section is to understand Iranian cyber actions and how they help to comprehend the regime's cyber strategy.

Operation Abadil is considered one of Iran's most destructive attacks and is part of a defensive strategy against the United States. The campaign launched in 2012 is still active and includes different versions and waves of DDoS attacks.[9] The first wave targeted the US financial system by attacking American banks, which were not prepared for such traffic at the time. The attack blocked the banks' websites and servers and prevented customers from using online banking services. Izz ad-Din al-Qassam Cyber Fighters, which are allegedly linked to the Iranian government, claimed responsibility for this attack. In this case, Iran utilized cyber force through a state-sponsored actor against one of its main enemies—the American financial establishment.

In 2012, the destructive malware, renamed "Shamoon," breached the Saudi Arabian oil giant Aramco and affected Saudi computer systems, causing great damage and recovery costs. Attacks against Saudi strategic targets and allies in the region, such as RasGas in Qatar, should be considered part of the Iranian defensive strategy in cyberspace.[10] In 2016, other versions of the malware attacked new targets, especially government ministries, such as the Ministry of Labor, and companies in Saudi Arabia, such as the

9 "Operation Abadil DDoS attack," *Radware*, https://security.radware.com/ddos-experts-insider/expert-talk/ddos-attacks-operation-ababil/.

10 "Operation Cleaver," *Cylance* (2014), 1–86.

Saudi Central Bank.[11] In 2018, new waves of the malware targeted critical industries (oil, energy, telecommunication) and government organizations throughout the region.

In May 2016, it was reported that an Iranian state-sponsored organization had used websites and servers to attack about 120 Israeli organizations and institutions;[12] later identified as the OilRig[13] hacker group, it has operated on behalf of the Iranian government since 2015. In May 2017, the same hacker group, using Russian-based attack tools, attacked computer systems belonging to an American contracting firm engaged in security.[14] The company's security experts noted that this was the first case of cooperation between Iranian and Russian hackers who sold their services at the highest cost. This attack also revealed a significant upgrade in the capabilities of Iranian hackers. A few months later, the US Treasury indicted the Ajily Software Procurement Group as an international crime organization. The Iranian-based group had used hackers to steal engineering software that could be used to design GPS-guided weapons from the United States and other Western countries.[15] This attack was part of Iran's defensive initiative against the economic restrictions imposed by the United States. Contrary to the previous cases discussed here, this case dealt with theft and business espionage and demonstrates how the Iranian government has used cyber force to circumvent US sanctions in order to import military technology.

In June 2014, it was revealed that an Iranian cyber terrorist group affiliated with the Iranian Revolutionary Guard Corps (IRGC) had been attacking hundreds of targets in Israel and the Middle East for about a year. The hacker group was called "Ajax Team" or "Rocket Kitten" and had been operating within the Iranian security organizations in recent years.[16] The multi-stage

11 Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage and Revenge* (Washington DC: Carnegie Endowment for International Peace, 2018), 1–57.

12 "Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford," *ClearSky*, January 5, 2017, https://www.clearskysec.com/oilrig/.

13 Bryan Lee, Robert Falcone, "Behind the Scenes with Oil Rig," *Unit 42*, April 30, 2019, https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/.

14 Nicole Perlroth, "Web Defenders Detect Russian Hand in Iranians' Hacking Attempt," *New York Times*, May 15, 2017, https://www.nytimes.com/2017/05/15/technology/web-defenders-detect-russian-hand-in-iranians-hacking-attempt.html.

15 "Ajily Software Procurement Group," *Iran Watch*, August 8, 2017, https://www.iranwatch.org/iranian-entities/ajily-software-procurement-group.

16 Check Point, *Rocket Kitten: A Campaign with 9 Lives* (2015), 1–38.

attack targeted a variety of channels, including Israeli scientists, embassy staff, NATO officials, Iranian dissidents, the Saudi royal family, and others. The purpose of the attack was to gain access and steal critical information. Experts estimated that this was a highly targeted, sophisticated, tenacious, and systematic attack system, based on intelligence gathering and focused information on the targets. In November 2015, the IRGC broke into the emails and social networks of members of former US president Barack Obama's administration, while Facebook confirmed that it had identified attempts to take over profiles of government employees.

ClearSky's cyber intelligence company published a report in July 2017 about an Iranian cyber intelligence operation known as "Wilted Tulip."[17] In this operation, the Iranian hackers known as "CopyKittens" managed to gain access to information from a number of government agencies in Israel.[18] The hackers used a variety of methods, including the Watering Hole attack, which involves breaking into news sites, infecting them, and sending links to various victims under the guise of legitimate articles in order to gain control of their computers. In order to gain the trust of the victims and make them click on the links to the infected sites, the group used a relatively complex and authentic network of profiles on Facebook, some of which had been around for years. To support the authenticity of those profiles, several websites (built with an Iranian website building platform) and business pages on the social network had been set up. Its victims included government agencies and private companies in several Middle Eastern countries such as Israel, Saudi Arabia, and Turkey, as well as Western countries, such as the United States and Germany.

In 2018, using a malware nicknamed "Madi," Iran attacked Israeli targets, in addition to US think tanks, companies, and academics, in order to steal information and documents from over 800 victims.[19] In November 2019, Microsoft declared that it had identified intense cyber activity by a hackers' group called "Phosphorous," allegedly linked to the Iranian government.[20]

17 Eduard Kovacs, "Iranian CopyKittens Conduct Foreign Espionage," *Security Week*, July 25, 2017, https://www.securityweek.com/iranian-copykittens-conduct-foreign-espionage.

18 Clearsky Security and Trend Micro, *Operation Wilted Tulip* (July 2017), 1–48.

19 GReAT, "The Madi Campaign – Part I," Kapersky, July 17, 2012. https://securelist.com/the-madi-campaign-part-i-5/33693/.

20 "Microsoft: Iranian Hackers Targeted a US Presidential Campaign," *Asharq Al-Awsat*, October 4, 2019, https://aawsat.com/english/home/article/1931446/microsoft-iranian-hackers-targeted-us-presidential-campaign.

This cyber operation targeted current and former US government officials, journalists, Iranians living outside Iran, and potential candidates for the 2020 US presidential election, although they were not specified. It consisted of more than 2,700 attempts to identify email accounts belonging to the specific targets, followed by attacks on 241 accounts.[21] This type of operation, which aimed to interfere in foreign election campaigns, has become a significant concern since the American administration concluded that Russia had succeeded in disrupting the 2016 election process. This attempt to disrupt foreign elections and to target people outside of Iran appears to be part of Iran's offensive operation.

Confronting Internal Adversaries

Despite recent calls to restrict access to the internet, Iran already implemented measures allowing the regime to control people's access to connectivity. Indeed, the government uses its control over the internet's access as a means of disrupting communication in the country, especially during times of popular unrest. Since 2009, each mass protest has led the regime to impose restrictions on internet access.[22] In November 2019, after the government announced a considerable increase in gasoline prices, civil protests exploded in Tehran and other cities; the Iranian security forces responded violently and repressively, and a nationwide shutdown of the internet was imposed for almost a week, which completely disconnected the Iranians. This protest was a relevant example of Iran's use of its power in cyberspace for internal purposes: preventing its population from communicating, organizing, sharing information, and protesting.[23] The authorities' efforts to block the internet and restrict people's access to communication platforms in general and to develop a national internet project have been amplified by attempts to limit the use of VPNs (virtual private network) among the population. For instance, the Iranian government has obliged web services to sign a pledge stating that the "establishment and distribution of VPN and proxy services"

21 "Microsoft: Iranian Hackers Targeted a US Presidential Campaign."

22 Borzou Daragahi, "Massive Iranian Internet Shutdown Could Be Harbinger of Something Even Darker to Come, Experts Warn," *The Independent*, November 30, 2019, https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html.

23 Amy Slipowitz, "The True Depth of Iran's Online Repression," *Freedom House*, December 2, 2019, https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

are forbidden.[24] In addition to trying to prevent people from using VPNs, Iran is apparently trying to create a national VPN regulating the access to the internet for each individual based on profession, according to a statement of Hamid Fattahi, the CEO of the government-owned Telecommunications Infrastructure Company (TIC), on November 11, 2019.[25]

Since 2005, the Iranian regime under President Khatami has been advocating the idea of a closed and national network.[26] Beginning in 2010, the project of creating a "halal internet" network for Iran was introduced, with the aim of upholding Iranian values and preventing foreign threats from entering the regime's network, while it would also enable the authorities to control internal actors and monitor potential dissidents.[27] This initiative appeared shortly after the disclosure of the Stuxnet attack and was seen as an effort to respond to the new risks and threats that Iran faced at the time. Despite skepticism of observers regarding the success of such a project, other countries decided to adopt the same tactic; Russia, for example, passed a law in November 2019 that enabled the state to create an internet for Russian users only, which is completely closed to external actors and controlled by Russian authorities, indicating the real motive of such a project.[28]

This "halal internet," also known as the Iran National Information Network (SHOMA), is developing within the context of increasing surveillance of the population on the internet.[29] Indeed, calls of Iranian officials for greater surveillance and restrictions of the internet are repeatedly heard, and President Rouhani is often targeted by conservatives who accuse him of being weak

24 "State-Developed VPN Would Determine Iranians' Internet Access Based on Their Job," *Center for Human Rights in Iran*, November 21, 2019, https://iranhumanrights.org/2019/11/state-developed-vpn-would-determine-iranians-internet-access-based-on-their-job/.

25 "State-Developed VPN Would Determine Iranians' Internet Access Based on Their Job."

26 Julie Kebbi, "Internet: l'Autre repression du régime iranien," *L'Orient-le-jour*, November 22, 2019, https://www.lorientlejour.com/article/1195979/internet-lautre-repression-du-regime-iranien.html.

27 Christopher Rhoads and Farnaz Fassihi, "Iran Vows to Unplug Internet," *Wall Street Journal*, May 28, 2011, https://www.wsj.com/articles/SB10001424052748704889404576277391449002016.

28 Lucie Bras, "Russie: à quoi va ressembler le « Runet », le nouvel internet 100% russe contrôlé par Moscou?," *20Minutes*, November 5, 2019, https://www.20minutes.fr/high-tech/2644575-20191105-russie-quoi-va-ressembler-runet-nouvel-internet-100-russe-controle-moscou.

29 Amy Slipowitz, "The True Depth of Iran's Online Repression," *Freedom House*, December 2, 2019, https://freedomhouse.org/blog/true-depth-iran-s-online-repression.

and not responsive enough to the evolving threat that the internet poses.[30] For example, Attorney General Mohammad Jafar Montazeri called in May 2019 for stronger surveillance and more restrictions of the internet. He directly warned Minister of Information and Communications Technology Mohammad Javad Azari Jahromi,[31] apparently seen as too reformist, that he should be held accountable for delays in implementing new reforms and for not launching the "national internet" as desired by the Supreme Leader Ali Khamenei.

In parallel to the multiple restrictions that Iran has placed on foreign communication giants such as Telegram (messaging service application), the regime has helped to develop alternative platforms by providing technical support and financial resources to Iranian messaging applications Soroush and Bale, which operate at the national level. An indication that Iran was willing to foster the creation of local apps was in 2017 when it launched grant incentives of more than $200,000 USD for software developers able to reach a million users on their communication platform.[32] Government bodies benefit from weak data privacy policies that enable them to collect and store users' data, representing a potential danger for customers.[33] As the Iranian regime uses its power to regulate the use of the internet among the population, it both censors the internet and creates alternatives to exercise a strengthened control over it.

Analysis of the Iranian Cyber Operations and Force Build Up

Since the end of the 2000s, the developments of cyber risks and threats against the Islamic regime have fueled Iranian interests in cyberspace. Iran has invested a significant amount of resources to operate in cyberspace—

30 "En Iran, la justice appelle à davantage de surveillance sur Internet," *Le Monde*, May 4, 2019, https://www.lemonde.fr/keyhani/article/2019/05/04/en-iran-la-justice-appelle-a-davantage-de-surveillance-sur-internet_5994643_5470831.html.

31 "Iran Prosecutor Warns Minister to Tame Social Media or Face Consequences," *RadioFarda*, May 5, 2019, https://en.radiofarda.com/a/iran-prosecutor-warns-minister-to-tame-social-media-or-face-consequences-/29922128.html.

32 "In Iran, State-Sanctioned Messaging Apps Are the New Hallmark of Internet Nationalization," *Global Voices*, October 24, 2018, https://advox.globalvoices.org/2018/10/24/in-iran-state-sanctioned-messaging-apps-are-the-new-hallmark-of-internet-nationalization/.

33 "Pressure on Web Service Providers in Iran to Ban Proxies," *BBC Persia*, November 23, 2019, https://www.bbc.com/persian/iran-50531178.

which it refers to as an active battleground against the United States and its allies—and advances on multiple paths simultaneously: both to protect the regime against Western cultural attack and to physically destroy Western infrastructures.[34] The regime leads retaliatory operations against enemies that supposedly try to attack Iran, activities of cyber espionage to gain information on its adversaries' activity and capabilities, and offensives to disrupt them. At the eighth national civil defense forum held in Tehran in November 2019, the head of Iran's Civil Defense Organization, Brigadier General Gholamreza Jalali, announced that Iran was adopting a new defensive approach to the new hybrid and multi-layered threats and was developing defensive products to be used in cyberspace.[35]

The development of the cyber field signifies technological innovation and the strengthening of Iran's position in the international system as a regional technological power. The numerous resources that the Tehran regime invests in cyber have also born fruit in the civilian sector, while expanding the country's communications infrastructure to rural areas and increasing the speed of surfing in urban areas. The targets of Iran's cyberattacks are the regime's rivals inside the country, as well as its adversaries in the West and in the Middle East, including Israel and Saudi Arabia. Many of the targets are civilian-related organizations, such as security systems, private companies, academic actors, government officials, and public infrastructures. As in previous years, the Iranian cyberattacks continue to be effective due to the high level of planning of the operations and the systematicity in which they are carried out. Although the Iranian attacks are not technologically sophisticated, the technical level of the attacks has increased significantly in recent years.[36]

The following section will identify four main patterns that characterize the Iranian strategy in cyberspace. The first consists of a tit-for-tat strategy in terms of cyber defensive and offensive activities based on geopolitical developments as a pattern of the offensive operations against external adversaries. The second consists of developing internal cyber capabilities

34 Author's opinion based on research.

35 "Iran Opts for New Civil Defense Approach to Confront US Threats," *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

36 Ben Schaefer, "The Cyber Party of God: How Hezbollah Could Transform Cyberterrorism," *Georgetown Security Studies Review*, March 11, 2018, https://georgetownsecuritystudiesreview.org/2018/03/11/the-cyber-party-of-god-how-hezbollah-could-transform-cyberterrorism/.

in order to build an economic resilience; that is, being part of the world economy despite international sanctions and participating in technological innovation. This will be categorized as a pattern of the Iranian internal strategy in cyberspace with both offensive and defensive initiatives. The third aspect of the cyber strategy corresponds to the regime's set of values, religion, and cultural rules, as part of an offensive and defensive strategy applied both internally and externally. Finally, the fourth characteristic could be explained as the full exploitation of both the cyber toolkit and the lack of a legal framework distinguishing cyber from other fields of activity, enabling Iran to strengthen its offensive strategy against internal and external adversaries.

Tit-For-Tat Strategy of Adapting to the Geopolitical Context

Soon after the disclosure of the Stuxnet virus, Iran accelerated its pursuit of its operation in cyberspace. Two years later, the US economic sanctions led the Islamic Republic to attack its American rival in the cyber field. Iranian strategy in cyberspace should be considered a tit-for-tat strategy as it adapts its responses to geopolitical tensions at a regional or international level as part of its external offensive strategy in cyberspace. The use of offensive activities in cyberspace to respond to geopolitical events has been a steady mechanism in Iran. This trend means that Iranian cyber strategy is linked, if not dependent on, its geopolitical interests and adapts the strategy to them. This is an interesting element in comprehending Iranian cyber strategy as other countries do not especially design their cyber strategy in response to geopolitical developments (for example, China or Russia).[37]

The United States considered Operation Abadil as the most significant attack allegedly launched by Iran in order to counter US-imposed international economic sanctions following the development of Iran's nuclear program. This attack was considerable, given the level and intensity of the attacks. In 2016, the US Department of State indicted seven Iranian individuals, who were linked to the Iranian Revolutionary Guard Corps for participating in the attack.

The characteristic of Iran's adapting its cyber strategy to geopolitical developments has been observed in the negotiations for the Joint Comprehensive Plan of Action (JCPOA). US officials commented that Iran conducted cyber

37 Mark Pomerleau, "DoD Releases First New Cyber Strategy in Three Years," *Fifth Domain,* September 18, 2018, https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy/.

operations that caused significant damage to companies in the West and to Iran's enemies in the Middle East in 2013 and 2014, the period leading up to the agreement.[38] A clear increase in the number of Iranian offensive attacks in cyberspace can be discerned when sanctions were applied, while the JCPOA had a real impact on Iran's cyber strategy as the frequency and scale of attacks decreased with the nuclear deal's signature. When President Trump announced his decision to withdraw from the JCPOA in May 2018, it had the opposite effect. Less than twenty-four hours later, Iran had launched an aggressive campaign of phishing emails sent to US allies abroad. The level of preparation needed for this attack indicated that the Iranian forces had actually prepared the attack before Trump's announcement and chose to undertake the operation as a response to his decision. Indeed, experts identified a resurgence of cyber offensive activities coming from Iran, signifying a real shift in policy.[39] According to cybersecurity experts, Iranian efforts to target American facilities and individuals in cyberspace intensified after 2018 and following the US withdrawal from the JCPOA.[40]

Iran's activities outside the country through the support of proxies should also be included in this tit-for-tat strategy. The second wave of the Shamoon operation in 2016–2017 included references to Yemen and an image of the Syrian child Alan Kurdi appeared on targeted devices and was observed as retaliation for Saudi activities in Syria and Yemen. Recently, in June 2019, CrowdStrike and FireEye also stated that Iranian offensive cyber operations had intensified.[41] This offensive came shortly after the Trump administration imposed new sanctions on the Iranian petrochemical sector. According to CrowdStrike, "Refined Kitten," —the hackers' group that is thought to have instigated this cyber offensive—has been targeting the American defense and energy industries for years. In September 2019, Iran was accused of undertaking the attack against Aramco; however, Iran denied it and accused

38 Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks," *Foreign Policy*, October 2, 2017, https://foreignpolicy.com/2017/10/02/abandoning-iranian-nuclear-deal-could-lead-to-new-wave-of-cyberattacks/.

39 Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks," *New York Times*, May 11, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html.

40 "Iranian Hackers Wage Cyber Campaign amid Tensions with US," *Asharq Al-Awsat,* June 22, 2019, https://aawsat.com/english/home/article/1779921/iranian-hackers-wage-cyber-campaign-amid-tensions-us.

41 "Iranian Hackers Wage Cyber Campaign amid Tensions with US."

the Houthis (Zaydi Shiites in Yemen).[42] This attack had a significant impact on the largest oil producer and delayed oil production. It happened just after US officials declared they attacked Iran in a covert campaign in June 2019.

Building a Resilience: Circumventing Economic Pressure and Leading a Cyber Revolution

Despite the creation of new cyber bodies and implementation of cyber regulation, the Iranian government seemingly invests in the education of future generations[43] as part of an offensive strategy aiming to build internal cyber capacities. Iran has massively invested in the cyber field by creating new official organizations and infrastructure and a considerable part is also dedicated to education. The government, as well as non-state actors, apparently recognize the importance of educating people in cyber; for example, several Iranian universities offer hacking classes.[44] Educating a large number about cyber technology is likely to support the industry's development and perhaps to enhance people's commitment to the state in this field.[45] Since attribution is difficult in cyberspace, unofficial state-related groups can operate on behalf of the interests of the state. Iranian decision makers realized the significance of this phenomenon, of investing large amounts of money to educate people, with the expectation that they would eventually commit to supporting the state. Although the investment in education will not systematically be translated into new public employees, it could lead to the formation of self-motivated groups. In addition, the government has shown interest in supporting start-ups and innovation. In September 2019, the Iranian government decided to invest $225 million USD in the Iran Innovation Fund for supporting innovation and encouraging start-ups.[46]

Developing its cyber capabilities to become a leader in cyberspace also implies that Iran engages in cyber espionage in order to steal rivals' technology and to gain information about their capabilities. The Madi malware in 2012,

42 Bruce Riedel, «Who are the Houthis, and why are we at war with them?» *Brookings*, December 18, 2017, https://www.brookings.edu/blog/markaz/2017/12/18/who-are-the-houthis-and-why-are-we-at-war-with-them/.

43 Veronika Netolická and Miroslav Mareš, "Arms Race 'in Cyberspace' – A Case Study of Iran and Israel," *Comparative Strategy* 37, no. 5 (2017): 414–429.

44 "Threat Intelligence Briefing Episode 11," *HP Security Research,* February 2014.

45 Netolická and Mareš, "Arms Race 'in Cyberspace."

46 "Iran Gov't Invests $225m in Innovation Fund," *Financial Tribune*, September 6, 2019, https://financialtribune.com/articles/sci-tech/99750/iran-gov-t-invests-225m-in-innovation-fund.

the Rocket Kitten activities in 2014, and the attempts of the Ajily Software Procurement Group to illegally import American stolen software to Iran are all relevant examples of Iranian cyber espionage activities. Iranian activities to gain technological power are usually accompanied by disruptive activities designed to target foreign critical infrastructures, especially in the energy and defense fields, as was illustrated by the APT33 threat actor (also known as Elfin) for many years.[47]

The development of cyber capabilities might also serve as a means of circumventing economic pressure and diversifying sectors of the economy as part of a defensive strategy. Indeed, building and improving cyber capabilities also means developing new technological tools. The cryptocurrencies, which are completely digitalized, could embody the economic tools of cyberspace. For now, crypto trading is still forbidden in the Islamic Republic, but cryptocurrency mining was recently authorized and legislated as an industrial activity.[48] Iran's Ministry of Industry, Mine, and Trade has the full authority to give approvals to local miners, and some rules were designed to regulate this activity. The new law was passed in Iran at a time when Iranians already operated crypto mining as a way of avoiding economic sanctions. Even if the law limits the geographical areas in which it is allowed to mine and obliges individuals to pay charges for the electricity consumed, Homayun Haeri, the deputy minister of energy, has declared that the government will vote on a measure to apply lower electricity rates for mining farms. This kind of measure is likely to foster mining activities in Iran. This pronouncement sounds suspicious, however, since the Central Bank has recommended banning the payment of cryptocurrencies within Iran, whereas civil society and companies have tried to promote cryptocurrencies at a domestic level. If Iran is developing this tool to counter international economic sanctions, the United States has already taken action against two Iranians who allegedly facilitated payments for the SamSam malware. The State Department Office of Foreign Asset Control put the two on its sanctions list for bitcoin activities, meaning they are blacklisted and cannot send money to individuals and

47 "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.," *Symantec*, March 27, 2019, https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage.

48 Marie Huillet, "Iranian Govt Authorizes Cryptocurrency Mining as Industrial Activity," *Coin Telegraph*, July 29, 2019, https://cointelegraph.com/news/iranian-govt-authorizes-cryptocurrency-mining-as-industrial-activity.

services or receive from them.[49] Furthermore, in December 2019, President Hassan Rouhani proposed the creation of a Muslim cryptocurrency as a mean of fighting against American economic hegemony. This was the first time the Iranian regime publicly announced it was creating cryptocurrency in order to avoid the use of the US dollar as part of a defensive financial strategy.[50]

Protecting the Regime's Stability and Spreading its Values

After the 2009 Green Movement, Iran realized the danger of new technologies in terms of organizing resistance and a potential rebellion. As the country reacted to this phenomenon, it developed a defensive and offensive strategy in cyberspace, applied both internally and externally. The regime tried to regulate activity in cyberspace and to control the content shared as part of defensive operations inside the country. According to a survey published in 2012, 27 percent of websites were then blocked in Iran,[51] as they were considered to be against Muslim values. Indeed, there is a national ban of most of the social networks, including Facebook and Twitter.[52] According to an interview with Prosecutor Ahmad Ali Montazeri, who presides over the Internet Censorship Committee, Iran banned 14,000 websites and social media accounts weekly in 2016.[53] He explained that the content of these websites, which opposed Iranian values and religion, justified their closure, adding that the country was under attack by foreign and hostile media. This victimization tactic has been used at times in Iran to apply censorship and spread propaganda. In 2017, 2018, and 2019, during the Iranian popular protests, the regime blocked some websites and communication platforms.

---

49 "US Regulators Tie Two Bitcoin Addresses to Iranian Ransomware Plot," *CoinDesk*, November 28, 2018, https://www.coindesk.com/us-regulators-tie-two-bitcoin-addresses-to-iranian-ransomware-plot.

50 Helen Partz, "Iran Wants to Create Crypto to Confront 'Economic Hegemony' of US," *CoinTelegraph*, December 19, 2019, https://cointelegraph.com/news/iran-wants-to-create-crypto-to-confront-economic-hegemony-of-us.

51 "Current State of Internet Censorship in Iran," *View DNS.info*, March 23, 2012, https://viewdns.info/research/current-state-of-internet-censorship-in-iran/.

52 Leyla Khodabakhshi, "Why Ordinary Iranians Are Turning to Internet Backdoors to Beat Censorship," *BBC News*, January 10, 2018, https://www.bbc.com/news/blogs-trending-42612546.

53 "Iran Bans 14 Thousand Websites and Accounts Weekly," *Al Arabiya*, December 8, 2016, https://english.alarabiya.net/en/media/digital/2016/12/08/Iran-bans-14-thousand-websites-and-accounts-weekly-.html.

The authorities even cut off internet access in some places.[54] For example, the government blocked Telegram, one of the most used communication apps among Iranians. Indeed, Iranian officials, who apparently learned from previous events, were willing to prevent civil society from communicating, informing, and organizing itself through this platform.

Maintaining Iran's culture is important for Iran in its drive to develop cyber capabilities and is a pattern of its strategy. The cultural factor is reflected in Iran's cyber activities, as many attacks led by Iranian actors have been linked in one way or another to religious or cultural justifications. Pride is also likely to be a reason why Iran wants to lead the region and the world in terms of technological innovation.[55] Jalali, the head of Iran's Civil Defense Organization, highlighted in November 2019 the prominent role that Iran has in the field of cyber, adding that the regime developed cyber defense before any other countries, including the United States, and that many countries, such as Russia and North Korea, were willing to receive training from Iranian cyber forces.[56] The sense of national pride related to the role of being a leader in the technology field is crucial to understanding Iran's strategy in cyberspace. Since around 2010, Iran has succeeded in expanding internet access to rural areas and to improving connectivity in cities,[57] making it one of the Middle Eastern countries with the largest number of internet users.

The regime is also committed to spreading its values outside the country, as part of an offensive operation against its "enemies." FireEye, a cybersecurity company, identified a campaign promoting Iranian political narratives in 2018.[58] The operation included the use of illegitimate news websites and the abuse of social media. The cybersecurity company analyzed it as a replication of Russian attempts to influence foreign public opinion during the 2016 US presidential election. In September 2019, Gholamreza Soleimani,

54 "In Response to Protests, Iran Cuts Off Internet Access, Blocks Apps," *NPR*, January 3, 2018, https://www.npr.org/2018/01/03/575252552/in-response-to-protests-iran-cuts-off-internet-access-blocks-apps.

55 Gawdat Bahgat and Anoushiravan Ehteshami, "Iran's Defense Strategy: The Navy, Ballistic Missiles and Cyberspace," *Middle East Policy Council* 24, no. 3 (2017): 89–103.

56 "Iran Opts for New Civil Defense Approach to Confront US Threats," *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

57 Anoushiravan Ehteshami, "Iran: Stuck in Transition," *Journal of International and Global Studies* 9, no. 2 (2017): 186–188.

58 Ed Parsons and George Michael, "Understanding the Cyber Threat from Iran," *MWR Info Security*, 17 April 2019, https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran.

commander of the Basij organization, announced the creation of one thousand cyber battalions around the country, via pro-regime user accounts on social media.[59] A battalion is composed of around five-hundred soldiers, meaning that the regime probably launched more than half a million pro-regime accounts. He stayed silent regarding the means and budget used by the Basij organization to achieve this project. Soleimani also stated that "the enemy has expressed concern over the organized presence of revolutionary youth in cyberspace on several occasions, and that reflects the momentum that has been created. This presence will expand and be enhanced." However, despite this new initiative aiming to spread pro-regime views on the internet, Iran is likely to face difficulties since Twitter has been removing thousands of state-backed accounts lately (including accounts believed to be linked to the Iranian government).

Besides Iran's determination to protect its system of values, the regime also has attempted to fight against foreign ideas and has spread its propaganda through cyberattacks. For example, during Operation Abadil, hackers demanded the removal of "Innocence of Muslims," a movie distributed in 2012 and considered as offensive to Muslims' honor.[60] The cyberattack was accompanied by a cultural vindication because Iran's image had been insulted. Another example of spreading propaganda through a cyberattack was the Shamoon malware attack in 2016. During this operation, infected devices were smeared with anti-Western images, such as an American flag burning. Another version of Shamoon later reappeared and spread the malware with a verse of the Quran in infected devices.[61]

Taking Advantage of Cyberspace's Characteristics

Cyberspace is a privileged area in which Iran and non-liberal countries do not play by the same rules as do democratic countries, such as the United States and Israel. Indeed, they do not submit to the same rules and Iran appears to take advantage of this difference in its offensive strategy against both

59 "Nouveaux cyber-brigades en Iran," *PressTV*, September 7, 2019, https://www.presstv.com/DetailFr/2019/09/07/605586/Des-cyberbrigades-en-Iran.

60 Kate Brannen, "Abandoning Iranian Nuclear Deal Could Lead to New Wave of Cyber Attacks," *Foreign Policy*, October 2, 2017, https://foreignpolicy.com/2017/10/02/abandoning-iranian-nuclear-deal-could-lead-to-new-wave-of-cyberattacks.

61 Charlie Osborne, "Shamoon Data-Wiping Malware Believed to Be the Work of Iranian Hackers," *ZDnet*, December 20, 2018, https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/.

internal and external adversaries. Since they do not adopt the same values, Iran considers some practices acceptable and others as ethically and morally forbidden. In contrast, the Western, democratic, and developed countries act according to the legal framework of their countries. They also tend to adopt and respect international law, because they greatly value the public opinion.

As a non-liberal regime, Iran allows itself to regulate and censor cyberspace in an extremely restrictive way, depriving its citizens of basic tools for connecting with the world. Information regarding national activities in cyberspace is also kept hidden from the public. While democracies generally avoid ambiguity, out of their duty to respect legal principles, it is fully used by authoritarian regimes such as Iran. Iran remains very opaque when it comes to cybersecurity and information activities, whereas democracies must remain highly transparent and will be held accountable for any kind of decision made. Rejecting the concept of accountability, Iranian officials benefit from wider freedom of action, without generally fearing the population's disapproval. This is especially the case when Iran attempted to infiltrate American and European networks through the operation led by the Phosphorous group, which was discovered by Microsoft in September 2019. Similar to Russian activities in 2016, Iran apparently has tried to influence foreign elections, attacking potential candidates of the 2020 presidential election.

The ambiguity and deniability of cyberattacks allow attackers to use cyber warfare via covert operations. It makes cyberspace a privileged area to confront enemies without fearing direct retaliation. The activity of hackers' groups whose links with the Iranian government are ambiguous is another issue. Cooperation with foreign groups is also an evolving phenomenon of Iran's cyber activities, which enables Iran's denial. Indeed, the OilRig's use of Russian cyber tools to attack an American target in 2017 illustrated the coordination between Russian and Iranian hackers. Another aspect of the deniability of cyberattacks is the importance of proxies through state or non-state actors that are supported by Iran and that conduct activities on their own in agreement with Iranian interests. Proxies of Iran are spread all over the region, both within Shiite and Sunni forces (Houthis in Yemen, Hamas in Gaza, Hezbollah in Lebanon, and so forth). Due to the ambiguity caused by the proxies' activity, Iran easily denies involvement in cyber operations, as it rejected the accusation of attacks against Saudi facilities in September 2019, claiming the Houthis' responsibility for this operation.

The last pattern identified as part of Iran's national cyber strategy is its deniability of being targeted by attacks. Indeed, public statements by Iranian government officials claiming that Iran is impervious to cyberattacks are common. A recent example of these declarations is in an interview with Jalali, published in November 2019, who said that foreign attempts to attack Iran in cyberspace had been unsuccessful for the past two years a result of the effectiveness of defensive cybersecurity mechanisms.[62] At the same time, US officials claimed the success of a covert cyber operation in Iran, which affected the regime's ability to target oil tankers in the Persian Gulf in June 2019.[63] In fact, Minister of Communications and Information Technology Mohammad Javad Azari Jahromi even declared that the United States "must have dreamt" about the operation.[64]

Conclusion

Iran currently poses a major cyber threat to the international system. The actions of the Islamic Republic and the strategy behind it have led Western government officials and experts from the private sector to believe that Iran seeks to stand alongside cyber powers, such as Russia and China. Should Iranian capabilities continue to evolve, experts say that an attack that could damage physical infrastructure is likely.

The offensive cyber strategy of Iran can be described as a tit-for-tat strategy, based upon cultural justification, pride, and benefits from cyberspace particularities. Iran has emerged among major global cyber actors. The reputation that the Islamic Republic has acquired serves its strategy and its efforts to use asymmetrical warfare against its external adversaries. The Iranian regime invests a great number of resources in developing the country's cyber capabilities in a variety of fields and subsequently strengthens its field of defense. This field also benefits from civilian investments where Iranian institutions such as Sharif University are highly regarded.

Iran's defensive strategy is led by its need to build economic and technological resilience as well as by its determination to neutralize internal and external threats. The regime recognizes the importance of establishing

62 "Iran Opts for New Civil Defense Approach to Confront US Threats," *Fars News Agency*, November 5, 2019, https://en.farsnews.com/newstext.aspx?nn=13980814000432.

63 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," *New York Times*, August 28, 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

64 Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say,"

defensive capabilities alongside attack capabilities. In addition, it invests great efforts in acquiring surveillance capabilities and monitoring internet activity in order to maintain government integrity, aided by expert attackers from its natural partnerships with China, Russia, and North Korea.

Analysis of recent cyberattacks attributed to Iran shows that the regime has targeted a wide range of enemies, including Iranian dissidents inside and outside Iran, its close neighbors, such as Israel and Saudi Arabia, and distant countries such as the United States and the European states. Even if it cannot be compared to the United States or Israel, Iran is improving its cyber capabilities. Iran's cyberattacks have become more focused over the past two years; they involve the use of a wide range of tools and methods and are clearly designed and executed with a high degree of professionalism and patience worthy of bridging the technological gaps and increasing their effectiveness. Whether Iran has benefited or lost in terms of its offensives efforts against its external adversaries requires a barometer of consensus, while indicators may include national and defensive infrastructure and the public rhetoric.