International Journal of Formal Sciences: Current and Future Research Trends (IJFSCFRT)
ISSN (Print) , ISSN (Online)

https://ijfscfrtjournal.isrra.org/index.php/Formal_Sciences_Journal/index

A Swift Look at the Iranian Cyber Program

Ali Al-Ghani*

Ghani Academia, Seri Kembangan, Selangor 43300, Malaysia
Email: alialghani98@gmail.com

Abstract

This paper attempts to clarify the objectives of the Iranian cyber program, the efforts made to develop it, and the capabilities of this program while presenting models of Iranian cyberattacks on Western and Arab institutions and highlighting the actors conducting cyber campaigns inside and outside Iran.

Keywords: Cyberspace; Stuxnet Attack; Iranian Cyber Threats.

1. Introduction

Iran was one of the first regional states to launch its presence in cyberspace since 1993 before others gained access to the Internet and electronic technology. Still, it soon began to look for ways to limit the free flow of information to curb freedom of expression. Thus, an e-government work, which first appeared in a network of online actors, has evolved in attempts to censor and interfere with what is written, spoken, or acted by opponents of the regime or activists on social media. Post-Shah Iran, however, has adopted a centralized control of information, created dedicated government ministries to oversee various media, and adopted strict rules that prohibit criticism of the Supreme Leader and his government. RSF's designation of Iran as one of the world's most repressive countries on press freedom often comes from the media [1]. Iran appears adept at building electronic networks worldwide, uses an inexpensive way to train and cooperate with proxies, and supports the electronic capabilities of its military arms in Lebanon, Yemen, Syria, and Iraq. Further, it has formed a variety of local agencies in charge of cyber affairs. Thus, it is a vital to analyze Iranian cyber program goals and threats from wide perspective. .

2. The Goals of Iran's Cyber Program

This Iran's cyber program has several goals focused on preventing another attack similar to the Stuxnet attack in 2010 that caused significant damage to Iran's nuclear reactors. It also avoids a hack on Iran's computers by viruses, such as Flame Virus struck in 2012, which wiped out its data. Kasper SkyLab has revealed that this virus can steal important information stored in computers as well as information in specific target systems [2].

---

* Corresponding author.

In the same vein, Iran seeks to rein in and frustrate online activities for local opposition parties and regime opponents, for whom cyberspace is an important communication platform for information dissemination and counteractivities [3]. In addition, the regime hopes to prevent the penetration of domestic cyberspace with Western ideas and information that are incompatible with Iran's vision. The lack of trust and continued confrontation between Iran and the United States is a crucial variable behind Iran's drive to develop intelligent systems fostering asymmetric power and preventing the international community from moving toward regime change. It believes that the U.S. soft war efforts to instill foreign ideas, values, and ideologies to undermine its regime threaten its resilience and have a more profound impact than the threat of military action. Self-reliance will liberate Tehran from international determinants that prevent it from acquiring advanced technologies while enabling it to develop inexpensive local military techniques that will have significant operational effects on the regional and global competitive landscape. Iran's geopolitical position is mainly present in a region where competing and sometimes conflicting international and regional interests are current. Moreover, Iran's strategy aims to expand its power and enhance its regional presence, avoiding severe restrictions on its conventional military capabilities. Concerning a report by the International Institute for Strategic Studies, international sanctions and restrictions on arms imports have made it difficult for Iran to develop or purchase weapons that keep pace with military and technical developments [4]. Cyberwarfare is, therefore, an essential tool for amplifying Iran's power, strengthening its position, and exerting its influence at the regional and international levels. so in September 2013, several commanders from the army, navy, air force, air defense, Iran's Revolutionary Guard, and police forces were involved in the cybersecurity program at the Iranian Army's Command and Control University to train in hardware and software, and to counter, analyze, and prepare an appropriate response to cyber threats [5]. Iran has developed asymmetric responses such as ballistic missiles and drones, as well as pro-Iranian militias in Iraq, Syria, Lebanon, and Yemen, and built a cyber-piracy network to inflict enemy casualties and avoid confrontation on the conventional battlefield. Cyber-attacks are part of a continuum of conflict, said Iranian Revolutionary Guard Commander Hossein Salami indicated that in the atmosphere of a full-scale intelligence war with the United States, the front of the enemies of the revolution and the Islamic regime. This atmosphere combines psychological warfare, cyber operations, military provocations, public diplomacy, and scare tactics [6]. According to [7], the ambiguity, apathy, and evasions of potentially high-risk activities are often difficult to identify and correspond to some elements of Iran's technology-driven strategic culture, which enables it to manage these risks better. On this basis, it is difficult to quickly and convincingly claim responsibility for cyber-attack forensics is not based on sensory evidence in the traditional sense. So, Tehran can and, to some extent, deny that it did. The growth in size and complexity shown by Iranian cyber operators suggests that the threat from these groups continues to accelerate and that countering it requires new and innovative forms of digital defense. Cyber activism allows for the punishment and defamation of ideological rivals. Thus, Tehran has adopted it to launch retaliatory attacks against its enemies, particularly Saudi Arabia and the United States. Iranian pirates are believed to hold behind campaigns designed to disrupt a variety of U.S. government and private sector entities, including banks, hotels, and the U.S. presidential election. Such cyber operations may be designed to show strength and provide warnings to other countries or companies lobbying for Iran.

3. Future Forms of Tehran Cyber Attacks

Stuxnet is the world's first digital weapon targeted explicitly at Iran's nuclear enrichment facilities and has been successful in crippling it for nearly a decade [2]. It has spurred Tehran to engage in online activities and, in turn, has invested in military cyberinfrastructure, bolstered by Iran's personality perceptions and its capabilities that place it in the category of technological parity with developed countries. Since then, Iran has been accused of several cyberattacks. One of the most famous was the attack on the Saudi Aramco Oil Company in August 2012, when the virus "Shamoun" destroyed the data of about 30,000 computers [8].

The Ababil operation was followed as the administration imposed additional sanctions on the Central Bank of Iran and other entities, using distributed denial-of-service attacks to disrupt online banking programs. Although these attacks were rudimentary, Ababil was an effective targeting campaign that temporarily disrupted some of the commercial functions of a critical pillar of the U.S. economy and caused tens of millions of dollars in damage [9]. Although a group of hackers calling themselves the "Ezzedin al-Qassam Brigades Cyber Fighters" claimed responsibility for the Ababil operation, according to [9], the Iranian government has been instructed to do so. As part of the unveiling of this operation, the United States brought charges against seven Iranian infiltrators, accused of launching attacks on a group of American banks, which caused tens of millions of dollars in financial losses. Tehran was expected to increase its cyber activities after Qassem Soleimani's death. The U.S. cybersecurity experts warned of its reaction to his death, stressing the need for the United States to prepare for the possibility of audacious Iranian cyberattacks aimed at inflicting significant financial damage or threatening American lives in retaliation. Nevertheless, Tehran's cyber-attacks did not target any of the most critical installations such as oil institutions, transportation networks, or military command since such attacks would be carried out only once, given the difficulty of repeating the same attack method. Iran will not go for the option of a direct cyberattack that could lead to an armed response, something that Tehran, which tends to be pragmatic in most of its positions, avoids. So we are likely to see more covert attacks that are difficult to attribute to Iran directly. Yana Popkostova, director of the European Center for Energy and Geopolitical Analysis, believes that Iran is doing everything it can to prevent a direct military confrontation with the United States instead of trying to weaken its enemies with cyberattacks. Philip Ingram, a former colonel in the MI6, said in a similar vein, Iran has extensive and sophisticated range capabilities to target critical national infrastructure, financial institutions, educational institutions, manufacturers, and more. He warned that Iran has the capability to launch the first cyberattack [10]. To underscore the above, Iranian hackers, who called themselves "The Witch Cat" by impersonating a British professor and university researcher, violated a website of the School of Oriental and African Studies at the University of London; aimed at hacking some personal information about researchers and professors mainly from the U.S. and U.K. During the nuclear negotiations between 2013 and 2017, Iran engaged in a spying campaign, directed by the Iranian Revolutionary Guard, in which Iranian hackers infiltrated hundreds of universities, private companies, and agencies in the US and, overwhelmingly, stole more than 30 terabytes of academic data and intellectual property. Affected universities have spent about $3.4 billion on subscription services alone to access the data [4]. Tehran also targeted 13 personal e-mails of Treasury Department employees. Some belong to a Financial Crimes Enforcement Network director, which fights money laundering and terrorist financing. The others are used by the Office of Foreign Assets Control's (OFAC) licensing chief, who is responsible for enforcing U.S. sanctions [4].

5. Conclusion

In a In the light of the above, developments suggest the emergence of a new era of cyber-terrorism, whose interactions may not amount to the use of force or war but which seeks to achieve specific strategic or tactical effects affecting the behavior of hostile States. The cyber threats are a global phenomenon constantly evolving through well-organized networks with advanced capabilities and specialized work sections. These threats include propaganda and jamming of uncomfortable low-level web pages to espionage, severe disruption, and widespread infrastructure disruption. It could not be denied that Iran is developing its electronic power, which has become highly developed and mature. It requires counterpart Arab efforts to find an electronic strategy that matches Tehran's capabilities and create a joint research agenda with allies to confront Iranian threats and other actors in cyberspace. Therefore, there is a need for a strategic approach to cybersecurity that follows a comprehensive framework, focusing on building preventive and interactive cybersecurity capabilities and developing national talent and abilities.

Acknowledgement

Several actors have inspired me to write the paper. First and foremost, my sincere gratitude goes to Brigadier General; Abdullah Al-Ghani; without a hot discussion with him, I would not have achieved one of my biggest goals. Second, my appreciation goes to Mr. Ali Al-Husam for his cooperation throughout writing the paper. Lastly, a special thanks to IJFSCFRT for giving me a chance to publish this paper.

References

[1] A. Fixler and a. F. Cilluffo, "Evolving Menace Iran’s Use of Cyber-Enabled Economic Warfare," FDD Press, Washington, 2018.

[2] M. Holloway, "Stuxnet Worm Attack on Iranian Nuclear Facilities," 2015. [Online]. Available: http://large.stanford.edu/courses/2015/ph241/holloway1/. [Accessed 25 December 2021].

[3] G. Siboni, L. Abramski and a. G. Sapir, "Iran’s Activity in Cyberspace: Identifying Patterns and Understanding the Strategy," *Cyber, Intelligence, and Security,* vol. 4, no. 1, pp. 21-40, 2020.

[4] IISS, "Report launch: Open-source analysis of Iran's missile and UAV capabilities," 2021. [Online]. Available: https://www.iiss.org/events/2021/04/iran-missile-uav-capabilities-report-launch. [Accessed 25 December 2021].

[5] M. Baezner, "Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions," Center for Security Studies (CSS), Switzerland , 2019.

[6] K. Kausch, "Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East," *Policy Brief,* vol. 35, pp. 1-10, 2017.

[7] CRS, "Iranian Offensive Cyber Attack Capabilities," 2020. [Online]. Available: https://sgp.fas.org/crs/mideast/IF11406.pdf. [Accessed 27 December 2021].

[8] Z. Dehlawi and a. N. Abokhodair, "Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident," *Intelligence and Security Informatics (ISI)*, vol. 1, pp. 73-75, 2013.

[9] C. Anderson and a. K. Sadjadpour, "Iran Cyber Threats," Carnegie Endowment for International Peace, Washington, 2018.

[10] Q. Hodgson, L. Ma, K. Marcinek and a. K. Schwindt, "Fighting Shadows in the Dark Understanding and Countering Coercion in Cyberspace," 2019. [Online]. Available: https://www.rand.org/pubs/research_reports/RR2961.html. [Accessed 27 December 2021].