Cyberwarfare and Iran

Cyberwarfare is a part of Iran's "soft war" military strategy. Being both a victim and wager of cyberwarfare,[1] Iran is considered an emerging military power in the field.[2]

Since November 2010, an organization called "The Cyber Defense Command" (Persian: قرارگاه دفاع سایبری; *Gharargah-e Defa-e Saiberi*) has been operating in Iran under the supervision of the country's "Passive Civil Defense Organization" (Persian: سازمان پدافند غیرعامل; *Sazeman-e Padafand-e Gheyr-e Amel*) which is itself a subdivision of the Joint Staff of Iranian Armed Forces.[3]

According to a 2014 report by Institute for National Security Studies, Iran is "one of the most active players in the international cyber arena".[4] In 2013, a Revolutionary Guards general stated that Iran has "the 4th biggest cyber power among the world's cyber armies."[5][6]

According to a 2021 report by a cyber-security company, "Iran is running two surveillance operations in cyber-space, targeting more than 1,000 dissidents".[7]

NIN

Iranian cyber defense system - digital fortress part of national information network (national internet) - is developed for thwarting and attacks and engage attackers.[8]

Attacks against Iran

In June 2010, Iran was the victim of a cyber-attack when its nuclear facility in Natanz was infiltrated by the cyber-worm 'Stuxnet'.[9] Reportedly a combined effort by the United States and Israel,[10] Stuxnet destroyed perhaps over 1,000 nuclear centrifuges and, according to a *Business Insider* article, "[set] Tehran's atomic programme back by at least two years."[11] The worm spread beyond the plant to allegedly infect over 60,000 computers, but the government of Iran indicates it caused no significant damage. Iran crowdsourced solutions to the worm and is purportedly now better positioned in terms of cyber warfare technology.[9] No government has claimed responsibility for the worm.[11] The cyber-worm was also used against North Korea.

Events

- In October 2013, media reported Mojtaba Ahmadi, who served as commander of the "Cyber War Headquarters" was found dead wounded by bullets in Karaj.[12]
- November 2018: The Iranian telecommunication minister Mohammad-Javad Azari Jahromi accuses Israel of a failed cyberattack on its telecommunications infrastructure, and vows to respond with legal action.[13][14]
- October 2021: An attack paralyzed gas stations across the country, preventing users from purchasing fuel using state-issued cards and digital billboards displayed antigovernment messages

Attacks by Iran

The Iranian government has been accused by western analysts of its own cyber-attacks against the United States, Israel and Persian Gulf Arab countries, but denied this, including specific allegations of 2012 involvement in hacking into American banks.[11] The conflict between Iran and the United States has been called "history's first known cyber-war" by Michael Joseph Gross mid-2013.[15]

Events

- August 2014: An IDF official told press in that Iran has launched numerous significant attacks against Israel's Internet infrastructure.[16]

- 31 March 2015: There was a massive power outage for 12 hours in 44 of 81 provinces of Turkey, holding 40 million people. Istanbul and Ankara were among the places suffering blackout. According to *Observer.com*, Iranian hackers, possibly Iranian Cyber Army, were behind the power outage.[17]
- June 2017: The *Daily Telegraph* reported that intelligence officials concluded that Iran was responsible for a cyberattack on the British Parliament lasting 12 hours that compromised around 90 email accounts of MPs. The motive for the attack is unknown but experts suggested that the Islamic Revolutionary Guard Corps could be using cyberwarfare to undermine the Iran nuclear deal.[18]
- January 2022: The website of Israel's *Jerusalem Post* newspaper and the Twitter account of Maariv newspaper are hacked by suspected Iranian hackers. The website's content was replaced with a threat to target the Shimon Peres Negev Nuclear Research Center, and an apparent reference to Qasem Soleimani who was assassinated exactly two years earlier in Baghdad, Iraq.[19][20]
- March 2022: Large-scale cyberattacks were launched against multiple Israeli government websites, allegedly by Iran as retaliation for failed Mossad operations, though neither the attack attribution nor the purported Mossad operations could be confirmed as of March 2022. The National Cyber Directorate declared a state of emergency as a result of the attacks and unnamed defense sources told media outlets it was possibly the largest-ever cyberattack against Israel.[21][22]

Suspended Iranian accounts

On May 5, 2020, Reuters reported, quoting a monthly Facebook report, that Iranian state-run media had targeted hundreds of fake social media accounts to covertly spread pro-Iranian messaging, online since at least 2011, for secretly broadcasting online promotional messages in favor of Iran in order targeting voters in countries including Britain and the United States.[23] Accounts suspended for coordinated inauthentic behavior, which removed eight networks in recent weeks, including one with links to the Islamic Republic of Iran Broadcasting.[23]

See also

- Ashiyane
- List of cyber warfare forces

- Iranian Cyber Army
- Iran Cyber Police
- Communications in Iran
- Monica Witt
- Hybrid warfare against Iran
- Iran Mission Center

Alleged operations and malware against Iran

- Operation Olympic Games
- Stuxnet
- Flame
- Duqu
- Stars virus

Alleged operations and malware by Iran

- Foreign interference in the 2020 United States elections
- Mahdi
- Shamoon
- Operation Ababil
- Operation Newscaster
- Operation Cleaver
- Yemen Cyber Army
- Syrian Electronic Army

References

1. *Joshi, Shashank. "Iran, the Mossad and the power of cyber-warfare" (https://web.archive.org/web/20131003104343/http://blogs.telegraph.co.uk/news/shashankjoshi/100239562/iran-the-mossad-and-the-power-of-cyber-warfare/) . Archived from the original (http://blogs.telegraph.co.uk/news/shashankjoshi/100239562/iran-the-mossad-and-the-power-of-cyber-warfare/) on October 3, 2013. Retrieved March 18, 2015.*

2. *"Iran's military is preparing for cyber warfare" (http://flashcritic.com/irans-military-preparing-for-cyber-warfare/)* . *The Telegraph*. October 3, 2013. *Archived (https://web.archive.org/web/20180810114757/http://flashcritic.com/irans-military-preparing-for-cyber-warfare/)* from the original on August 10, 2018. Retrieved March 18, 2015.

3. Bastani, Hossein (December 13, 2012). *"Structure of Iran's Cyber Warfare" (http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3)* . *Institut Français d'Analyse Stratégique*. *Archived (https://web.archive.org/web/20190523162859/http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3)* from the original on May 23, 2019. Retrieved March 18, 2015.

4. Siboni, Gabi; Kronenfeld, Sami (April 3, 2014). *"Developments in Iranian Cyber Warfare, 2013–2014" (http://www.inss.org.il/index.aspx?id=4538&articleid=6809)* . INSS Insight. *Institute for National Security Studies*. *Archived (https://web.archive.org/web/20200105223245/http://www.inss.org.il/index.aspx?id=4538&articleid=6809)* from the original on January 5, 2020. Retrieved March 18, 2015.

5. *"Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World" (https://www.hackread.com/iran-biggest-cyber-army-israel/)* . Hack Read. October 18, 2013. *Archived (https://web.archive.org/web/20190530073522/https://www.hackread.com/iran-biggest-cyber-army-israel/)* from the original on May 30, 2019. Retrieved March 18, 2015.

6. *"- IRANIAN CYBER THREAT TO THE U.S. HOMELAND" (https://www.govinfo.gov/content/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm)* . www.govinfo.gov. *Archived (https://web.archive.org/web/20211028120955/https://www.govinfo.gov/content/pkg/CHRG-112hhrg77381/html/CHRG-112hhrg77381.htm)* from the original on 2021-10-28. Retrieved 2021-10-28.

7. *"Iran 'hides spyware in wallpaper, restaurant and games apps'" (https://www.bbc.com/news/technology-55977537)* . BBC News. 8 February 2021. *Archived (https://web.archive.org/web/20210807140602/https://www.bbc.com/news/technology-55977537)* from the original on 2021-08-07. Retrieved 2021-10-28.

8. *"شکست حملات سایبری در مقابل"دژفا"" (https://web.archive.org/web/20200209201319/http://newspaper.hamshahrionline.ir/id/62005/%D8%B4%DA%A9%D8%B3%D8%AA-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%D9%85%D9%82%D8%A7%D8%A8%D9%84%C2%AB%D8%AF%DA%98%D9%81%D8%A7%C2%BB.html)* . 2020-02-09. Archived from *the original (http://newspaper.hamshahrionline.ir/id/62005/%D8%B4%DA%A9%D8%B3%D8%AA-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%D9%85%D9%82%D8%A7%D8%A8%D9%84%C2%AB%D8%AF%DA%98%D9%81%D8%A7%C2%BB.html)* on 2020-02-09. Retrieved 2021-10-28.

9. *"Stuxnet and the Future of Cyber War". James P. Farwell and Rafal Rohozinski.*

10. *Sanger, David E. (1 June 2012). "Obama Order Sped Up Wave of Cyberattacks Against Iran" (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html)* . The New York Times. *Archived (https://web.archive.org/web/20120601112345/http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html)* from the original on 1 June 2012. Retrieved 1 June 2012.

11. *"US General: Iran's Cyber War Machine 'A Force To Be Reckoned With'" (http://www.businessinsider.com/us-general-irans-cyber-war-machine-a-force-to-be-reckoned-with-2013-1)* . Business Insider. *Archived (https://web.archive.org/web/20190402222626/https://www.businessinsider.com/us-general-irans-cyber-war-machine-a-force-to-be-reckoned-with-2013-1)* from the original on 2019-04-02. Retrieved 2017-11-14.

12. McElroy, Damien (October 2, 2013). *"Iranian cyber warfare commander shot dead in suspected assassination" (https://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html)* . The Telegraph. *Archived (https://web.archive.org/web/20191007044226/https://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html)* from the original on October 7, 2019. Retrieved March 18, 2015.

13. *"Iran accuses Israel of failed cyber attack" (https://www.reuters.com/article/us-iran-israel-cyber/iran-accuses-israel-of-failed-cyber-attack-idUSKCN1NA1LJ)* . Reuters. 5 November 2018. *Archived (https://web.archive.org/web/20200528133349/https://www.reuters.com/article/us-iran-israel-cyber/iran-accuses-israel-of-failed-cyber-attack-idUSKCN1NA1LJ)* from the original on 2020-05-28. Retrieved 2018-11-06.

14. *"Archived copy" (https://www.channelnewsasia.com/news/world/iran-accuses-israel-of-failed-cyber-attack-10900158)* . *Archived (https://web.archive.org/web/20190910160854/https://www.channelnewsasia.com/news/world/iran-accuses-israel-of-failed-cyber-attack-10900158)* from the original on 2019-09-10. Retrieved 2018-11-06.

15. *"Silent War" (http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business) Archived (https://web.archive.org/web/20141115153130/http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business)* 2014-11-15 at the *Wayback Machine* July 2013 *Vanity Fair*

16. Joeph Marks (22 April 2015). *"Iran launched major cyberattacks on the Israeli Internet" (http://www.politico.com/morningcybersecurity/0814/morningcybersecurity15035.html)* . Politico. *Archived (https://web.archive.org/web/20141110054322/http://www.politico.com/morningcybersecurity/0814/morningcybersecurity15035.html)* from the original on 10 November 2014. Retrieved 27 April 2015.

17. Micah Halpern (22 April 2015). *"Iran Flexes Its Power by Transporting Turkey to the Stone Age" (https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/)* . Observer. *Archived (https://web.archive.org/web/20191214152903/https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/)* from the original on 14 December 2019. Retrieved 27 April 2015.

18. *"Iran blamed for cyberattack on Parliament that hit dozens of MPs, including Theresa May" (https://www.msn.com/en-gb/news/uknews/iran-blamed-for-cyberattack-on-parliament-that-hit-dozens-of-mps-including-theresa-may/ar-AAtpPag?li=AAmiR2Z&ocid=spartanntp)* . The Telegraph. 14 October 2017. *Archived (https://web.archive.org/web/20171206135812/https://www.msn.com/en-gb/news/uknews/iran-blamed-for-cyberattack-on-parliament-that-hit-dozens-of-mps-including-theresa-may/ar-AAtpPag?li=AAmiR2Z&ocid=spartanntp)* from the original on 6 December 2017. Retrieved 6 December 2017.

19. *"Israel's Jerusalem Post Website Hacked" (https://www.reuters.com/world/middle-east/israels-jerusalem-post-website-hacked-soleimani-assassination-anniversary-2022-01-03/)* . *Reuters. 3 January 2022.*
20. *"Jerusalem Post website hacked with Iran warning on anniversary of Soleimani killing" (https://www.timesofisrael.com/israeli-news-sites-hacked-with-iran-warning-on-anniversary-of-soleimani-killing/)* . *The Times of Israel.*
21. *Yonah Jeremy Bob (2022-03-14). "Cyberattack against Israeli sites follows reports of failed Mossad op against Iran" (https://www.jpost.com/breaking-news/article-701269)* . *The Jerusalem Post. Archived (https://web.archive.org/web/20220314214405/https://www.jpost.com/breaking-news/article-701269) from the original on 2022-03-14. Retrieved 2022-03-14.*
22. *Yaniv Kubovich. "Israeli Government Sites Crash in Cyberattack" (https://www.haaretz.com/israel-news/.premium-israeli-government-sites-crash-in-cyberattack-1.10674433)* . *Haaretz. Archived (https://web.archive.org/web/20220314184356/https://www.haaretz.com/israel-news/.premium-israeli-government-sites-crash-in-cyberattack-1.10674433) from the original on 2022-03-14. Retrieved 2022-03-14.*
23. *"Facebook says it dismantles disinformation network tied to Iran's state media" (https://www.reuters.com/article/us-iran-facebook/facebook-says-it-dismantles-disinformation-network-tied-to-irans-state-media-idUSKBN22H2DK)* . *REUTERS. 5 May 2020. Archived (https://web.archive.org/web/20210821180131/https://www.reuters.com/article/us-iran-facebook/facebook-says-it-dismantles-disinformation-network-tied-to-irans-state-media-idUSKBN22H2DK) from the original on 21 August 2021. Retrieved 28 October 2021.*

External links

- Iranians Charged with Hacking IS Financial sector (https://www.fbi.gov/news/stories/2016/march/iranians-charged-with-hacking-us-financial-sector) (FBI)

Portals: Iran War Internet