Focus
January 2025

Cyber Threat Assessment in Iran: Advancement and Challenges

Syed Fraz Hussain Naqvi and Wardah Shahid

Cyber Threat Assessment in Iran: Advancement and Challenges

Syed Fraz Hussain Naqvi[*] and Wardah Shahid[**]

Abstract

Warfare strategies in the 21st century have evolved from kinetic means to the fifth generation of warfare that includes cyber warfare as well. Under this paradigm, states and non-state actors have used destructive malware to deter, disrupt, and destroy belligerent information systems. Thus, modern warfare aims at weakening the enemy from within, which is why regional and global superpowers have established a security firewall to protect from internal and external cyber-attacks. In this context, Iran owing to a series of security breaches from the US and Israel have used cyber warfare for strategic, geo-political, and tactical purposes. Its position in the Middle East and broader regional objectives compelled Iran to seek Russia and China's help in strengthening its intelligence system. Notwithstanding, the US in close cooperation with Israel has fortified its cyber landscape and mastered the art of offensive and defensive capabilities. Therefore, the conflux of cyber rivalries has not only escalated long-simmering tensions in the Middle East but has also for-casted a destructive cyber pandemic in the horizon. In this regard, This paper aims at highlighting Iran's evolution in

[*] Syed Fraz Hussain Naqvi is the Head of Iran Program at the Institute of Regional Studies, Islamabad.

[**] Wardah Shahid is an intern associated with the Iran Program at the Institute of Regional Studies, Islamabad.

> *the cyber domain and the perceived challenges in the form of espionage and malware attacks on its critical infrastructure.*

A Brief Overview of Cyber Warfare

Cyber warfare is an emerging non-traditional phenomenon used by nations and non-state actors to subdue the enemy by targeting its sensitive systems. This type of warfare impacts the general public as it involves hacking, spying, and breach of confidential data by a state or terrorist organisation in an attempt to weaken a potential adversary. The digital infrastructure, i.e., computers are used as a mean for cyber-attacks on civilian infrastructure, governmental institutions, and security installments. Therefore, espionage, sabotage, Denial-of-Service (DOS) attacks, propaganda, and surprise attacks are included in cyber warfare. In this regard, cyber wars for the most part are fought in shadows, but regardless of their subtle prevalence, they can strike an enemy with greater magnitude without it knowing.

Iran’s Cyber Capabilities

Iran with its strategic and geo-political position has redefined the terms of warfare by crossing an established threshold with regards to the global cyber landscape. Being at the forefront of cyber-attacks has reinforced the idea that intelligence gaps need to be secured through comprehensive reforms in the security sector. Upon Iran’s Supreme Leader, Ali Khamenei's discretion, the Council for Cyberspace was created in 2012 which provided a blueprint to ward off a multifront assault in the form of domestic dissidents and international foes.

Since then, rigorous scientific research by Iran's tech institutes, communication, and security companies have updated its once victimised role to a somewhat intimidating one. It has expertly capitalised on cyber warfare to advance its influence in the West Asian region as a hegemonic regional power. In this regard, it has countered adversaries like the US, Israel, and Saudi-Arabia by combining conventional warfare strategies with that of the cyber toolkit. This is further deliberated upon by former US Representative Peter Hoekstra (R-Michigan):

> *"Iran has boosted its cyber capabilities in a surprisingly short amount of time and possesses the ability to launch successful cyber-attacks on American financial markets and its infrastructure"*[1]

It has developed its defensive and offensive capabilities to ward off internal and external threats. Henceforth, Iran's defensive posture is limited to protecting sensitive data and vulnerable public utilities, while its offensive capabilities are situated around means and measures to eliminate enemy attacks. Therefore, without any formal cyber doctrine, the country considers asymmetric warfare, i.e., cyber-warfare to be its saving grace in the current realist world paradigm.

Strategic Objectives of Iran's Cyber Capability

Iran's conventional capabilities were unsuccessful in nullifying Western demands and restrictions. Therefore, its preoccupation with cyberspace is to achieve its original objectives of economic relief and developing its nuclear program. In this regard, firstly, Iran aspires to create a security firewall or more importantly a *'technological envelope'* aimed at cushioning sensitive information breaches.[2] Secondly, it wants to flex its regional muscles over adversaries, i.e., Israel and Saudi Arab while also dismantling their operational capabilities concerning economic, defense, and financial institutions. Thirdly, proxy forces such as Houthi rebels and Hezbollah have also been introduced to the cyber loop, thus symbolically monitoring the regime's political opponents. Fourthly, in the era of information warfare, cyber warfare has enriched Iran's deterrent capacity by psychologically harming arch-rivals through disinformation campaigns aimed at manipulating public opinion, weakening social cohesion, and influencing political outcomes. Lastly, due to its effectiveness and low cost, cyber warfare has provided Iran with a rudimentary solution to attack targets without any aggressive military campaign.

Iran's Cyber Capability Infrastructure

Iran's cyber offensive and defensive capabilities are embedded within the government, non-government, and military administrative structure. In this regard, the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence (MOIS) are operating at the front line. A detailed hierarchy is outlined below:

1. Islamic Revolutionary Guard Corps (IRGC)
2. The main body which oversees offensive cyber operations. Its *Electronic Warfare and Cyber Defence* wing monitors online content and supervises courses in cyber defense. Moreover, the IRGC also trains a paramilitary force called the *'Basij Cyber Council'* tasked with cyber-related services.[3]
3. Ministry of Intelligence (MOIS)
4. This governmental entity focuses on external and internal surveillance operations. It uses espionage and sabotage techniques against rival governments' energy,

telecommunications, and maritime transportation. Overall, this body retrieves signals intelligence from electronic communications.

5. The Cyber Defense Command.
6. The command's function is to protect national facilities from cyber intrusion, therefore its operations lay in the defensive domain.
7. The Iranian Cyber Army
8. This unit is comprised of technical experts and hackers tasked to carry out cyber-attacks on opponents in affiliation with the IRGC-cyber force.
9. National Cyberspace Center (NCC)
10. This institute is linked to the 'Supreme Council of Cyberspace'. Its purpose is the development of internet protocols and in some cases waging 'cultural war' against belligerents.
11. National Passive Defence Organization (NPDO)

The organization culminated in 2003 as a means to neutralize foreign cyber-attacks thus protecting national infrastructure.[4] It is mostly preoccupied with coordinating Iranian military strategies and improving its defense infrastructure. Since 2015, it has been headed by Brigadier-General Gholamreza Jalali Farahani.[5]

12. Iranian ATP Groups
13. Iran's state-backed *'Advanced Persistent Threat'* (APT) groups constitute cyber war activities against enemy states. Prominent APT groups such as *'Charming Kitten, Helix Kitten, Flying Kitten, Rocket Kitten, Muddy Water, and Shamoon Group'* are persistent in carrying sophisticated cyber-attacks against adversaries.[6]

14. Mabna Institute
15. The Mabna Institute was established in 2013 containing proxy contractors working for the Iranian government and the IRGC in conducting cyber operations.[7] Their activities include stealing authorised data and research materials from international universities, state agencies, private companies, and non-governmental organisations. Notable cyber activities include an attack on 320 universities and 50 private companies in 2016 and an attack of similar stature in 2018 whereby the Iranian suspects (association with Mabna Institute) were apprehended for digital fraud by the United States District Court for the Southern District of New York.[8]

Cyber Operations against Adversaries

Iran's cyber capabilities can be identified through deadly cyber-attacks it has launched against rival forces. In June 2015, Israel and Saudi Arabia identified Iranian involvement in a phishing campaign targeting 500 academic researchers.[9] By April 2017, the Iranian-affiliated hacker group *'OilRig'* had carried out cyber-attacks against 250 targets in Israel.[10] In April 2020, disruptions occurred in Israeli Water Authority systems, attributed to Iranian hackers. Moreover, in March 2021, the Iranian ATP group *'Charming Kitten'* targeted two dozen medical professionals in Israel and the US. By October 2021, Microsoft reported an alleged Iranian hacker attack against US and Israeli defense companies and transportation companies in the Middle East. Furthermore, the notorious *'Cyber Av3engers'* (hacker group) of Iran managed to breach multiple American organisation in December 2023 causing irreparable damage.[11] Most recently, in

April 2024, a report by Israel's National Cyber Directorate indicated a 43 per cent surge in cyber-attacks by Iran and Hezbollah over the past year.[12] These attacks indicate that Iran has been successful in going toe to toe with adversaries far humongous in cyber infrastructure.

Iran's Cyber Collaborations

Iran has been seeking Russia and China's assistance in the cyber domain to showcase a substantial show of force. This is attributed to its commitment to greater cyber excellence in the future.

Russia

In addition to conventional military and strategic convergence between Iran and Russia, the growing cyber security partnership has had the West gearing up for an impending confrontation. Russia has been steadily supplying nation-state-level cyber capabilities to Iran in what is labeled as an authoritarian partnership. Therefore, cyber collaboration is rooted in two uniform interests. Firstly, providing Iran with cyber tools against common enemies such as the US can incentivise joint espionage activities garnering information deemed crucial for both states.[13] This can, not only limit operational costs for both states but also augment flexible Russian cyber net across allies and adversaries alike. Adding on, in a surprising twist of affairs, the Russians are not keen on exposing their backs to Iran, therefore the main purpose behind sharing intelligence gains is keeping a close eye over Iranian intelligence operations.[14] Therefore, Russia is a key ally in Iran's cyber operations as it has previously supplied covert software and monitoring equipment to Iran which were used in state crackdowns against political opponents.[15] Though such tools are not necessarily malware-induced, they still encourage innovative insight into the cyber arena.

Furthermore, formal associations can be highlighted through the *'Information and Cyber Agreement'* in 2021, which was inspired by an earlier accord of 2015, centered on cyber defense capabilities. The 2021 agreement was signed between Iranian Foreign Minister Javad Zarif and Russian Foreign Minister Sergei Lavrov consisting of nine articles acknowledging future information security cooperation while strengthening cyber threat capabilities.[16] The agreement not so long ago, i.e., in December 2023 received a parliamentary nod by Iran, thus further fortifying the growing Iran-Russia relations in the cyber domain.[17] Subsequently, in March 2023, Russia dispatched a highly sophisticated digital arsenal used for the Iranian regime's surveillance activities.[18]

That being said, mutual dependence does not entirely hinge on a one-way partnership, Iran has been increasingly delivering military tools, i.e., Iranian drones and ammunition to Russia for its use in the Ukraine war.[19] Therefore, both Iran and Russia are in their ways trying to avail maximum gains from their defense union which has undoubtedly accelerated to a more robust partnership.

China

Iran and China's cyber relationship, though in its infancy has the potential of converting into something more indestructible. Alternatively, the Chinese have signaled a partnership with Iran to ward off the US and its ally's cyber hegemony. In this regard, in 2019 representatives from both sides openly acknowledged the necessity of cyber cooperation to counter Western threats.[20] Therefore, the Sino-Iranian partnership is found within China's assistance in the digital sphere through geo-location technologies, espionage, and data interception systems. These monitoring tools are provided by Chinese corporations such as *'ZTE and Tiandy Technologies'*, which are of substantial support to Iran's surveillance and indirect cyber activities.[21] In this regard, the *'Iran-China 25-Year Cooperation Plan'* in March 2021 is a 400 billion dollar venture by China in the areas of telecommunication and technology.[22] Under the technological field, the growing bilateral partnership extends to areas of artificial intelligence, 5G programs, cyber security, and information exchange between educational and technological companies.

China's heightened footprint in the Middle East, in the form of mediation or cooperation agreements (Saudi-Iran Rapprochement and Hamas-Fatah reconciliation), has encouraged it to play a more decisive role in its geo-politics. Coupled with its soft power sway as mentioned above, there are apprehensions of China's assertiveness by the US, as it will not only add more fuel to the bilateral tensions but also tip the regional balance of power.

Therefore after the detailed explanation, one last question remains, and that is will Iran, China, and Russia engage in a trilateral cyber partnership? The answer lies in the strategic interest of each state, which surprisingly coincides with limiting Western domination and threatening alliances like that of the US and Israel. In this regard, ostracised nations will continue to pose challenges to the Western mainstream. It might have crossed a possible cyber threshold, as there is a warning issued by *'Microsoft*

Threat Analysis Center', indicating a tripartite move by Iran, China, and Russia in influencing the November 2024 US elections.[23]

Cyber Attacks against Iran

Iran's posture as a growing cyber power does not eliminate the historical victimization it has perceived by challengers such as the US and Israel. In this regard, the first instance of real-world damage is showcased through the *'Stuxnet'* attack in 2010 generated by US-Israel intelligence agencies in a bid to target Iran's nuclear program. A computer worm was introduced in Iran's Bushehr nuclear power plant which quickly spread to 14 other facilities.[24] The aforementioned worm corrupted the engines attached to IR-1 centrifuges increasing its speed, thus leading to an explosion.[25] The damage caused was irreversible as according to the Institute for Science and International Security around 1000 centrifuges of the 9000 at the Natanz facility were demolished.[26] Furious by the attack, Iran carried out investigations which pointed fingers towards its arch nemesis US and Israel.

The 'weapon with extensive effects,' i.e., Stuxnet was a watershed moment quickly followed by the *'Duqu Virus'* in 2011 which contaminated the Iranian industrial and security sector with special emphasis on disrupting its critical nuclear talks. Subsequently, the *'Flame Virus'* in 2011 and a sophisticated *'Viper Attack'* were instances where the US and Israel used spy-destructive malware to subdue Iran.[27] The former stole critical information from a victim's server while the latter dismantled Iranian information and infrastructure systems, thus causing irredeemable damage. These miscellaneous operations can be reconciled under the US-Israel cyber partnership against Iran which manifests from Iran's nuclear technology and broader regional motivations.

United States - A Traditional Challenger

The US has been a famous proponent of spearheading a 'cyber sabotage' campaign against Iran, particularly impacting its nuclear and industrial networks.

Its advent was witnessed in 2006 in a clandestine operation nicknamed *'Olympic Games'* by then-President George W and continued well in the presidency of Barack Obama.[28] The US cyber-operation was initiated by the National Security Agency (NSA) and the Central Intelligence Agency (CIA) in collusion with Israeli intelligence. The idea is to manufacture malware to compromise the Iranian digital system by planting it in its computer networks. The overall campaign outlook resonated with a covert operation called *'Nitro Zeus'*, which ran parallel to the original plan.[29] The context of Nitro Zeus was to inflict an offensive and kinetic cyber-attack targeting the Iranian nuclear facility of Fordo, Iranian air defense, communications, and power grids. The plan was to receive a green signal if the nuclear negotiations initiated in 2013 failed to achieve its intended purpose of shackling Iran from enriching more uranium.[30] In this regard, the project could have completely paralysed the Iranian nuclear infrastructure, had the Stuxnet incident not taken place. Being a part of the project, the disclosure of the cyber-attack alerted the Iranians, who immediately enhanced their mitigation strategies against the cyber arch-rivals. Despite, a short-term implementation, the project was a turning point in the growing cyber war between Iran and its foes.

Being a tier one power allows US the leverage to carry out covert cyber-attacks with 0-day malware.[31] With this, bodies like the Department of Homeland Security (DHS), the Department of Defense (DOD), the National Security Agency (NSA), and the US Cyber Command (USCYBERCOM) have undertaken cyberspace campaigns to:

> "…limit, frustrate, or disrupt adversaries' activities below the level of armed conflict and to achieve favorable security conditions."[32]

Notwithstanding, the Pentagon has acknowledged the parameters of *'persistent engagement ' since* 2018 against antagonists.[33] This asserts that the US Cyber Command can carry out cyber-attacks against antagonists like Iran without official authorisation. Therefore, in the realm of cyberspace, Iran cannot yet match the US counterintelligence techniques which are encapsulated with foolproof cyber infrastructure.

Israel - A Regional Challenger

The regional belligerent Israel has also adopted the sphere of cyber warfare for monitoring the hostile activities of enemies. Being a close ally of the US, it has strived for information cooperation between the two countries in the domain of cyber warfare. In this regard, Israel has upped the ante by establishing a *'Specialized Cyber Unit'* and an *'Israeli National Cyber Directorate'* in 2015 to increase its capacity building in defensive and offensive cyber warfare. Moreover, entities like *'The Israeli National Cyber Security Authority* (NCSA) in 2016 and its first-ever *'National Cyber Security Strategy'* in 2017 aim to expand their intelligence base concerning insulation from enemy threats while giving them an edge to carry preemptive attacks against opponents.[34]

Nevertheless, Israel's security doctrine follows the principles of deterrence, resolution, warning, and defense.[35] Israel has carried spades of attacks on adversaries using government, non-government, and hacking groups such as:

1. **Unit 8200**: The Israel Defence Force Unit 8200 was created in 1948 by a notorious group of computer engineers tasked with gathering information under the shrouds of research and technological development.[36] In this regard, it regularly targets Iranian facilities amongst which is the development and testing of the infamous Stuxnet attack which was set in motion in collaboration with the CIA.[37]
2. **Pegasus Spyware:** The Pegasus spyware is the world's most powerful cyber weapon as it can retrieve data from the victim's smartphone without it accessing any links or files.[38] This surveillance tool is not only used by Israel against potential enemies but is sold to foreign government agencies (18 reported client countries) who use it to collect information against domestic and external opponents.[39]
3. **Cellebrite:** The Israeli digital intelligence firm was created in 1999, whose prized products i.e. the *'Universal Forensic Extraction Device'* (UFED) and the *'Physical Analyzer'* are sold to law enforcement agencies around the globe for data theft under the pretense of data analysis and extraction.[40] It plays a similar role as that of the Pegasus spyware and is therefore implicated in heightened human rights abuses.

4. **Israeli Elite Force**: The Israeli Elite Force, a hacktivist group, now redundant was established in 2013 with the express aim of carrying out cyber operations and online vandalism against adversaries such as Iran.[41]

Conclusively, Israeli and American cyber warfare campaign against Iran has fulfilled its benchmark of information warfare via propaganda apparatus and public opinion management. Moreover, it has ruptured Iran's electronic and security protocols by appropriating critical information and dismantling sensitive systems. They have utilised sophisticated tactics such as website defacement, data breach and theft, and destructive attacks, thus targeting sensitive data and disabling computer logistics.

Cyber Geo-Politics in the Middle East

The Middle East region has been ripe with protracted conflicts encouraged by hegemon states, proxy forces, and global superpowers. Geo-political tensions and regional stability have achieved new heights under the current state of affairs. In this case, the rapid digitisation by security states such as Iran and Israel has added a new dimension to contemporary warfare. A cyber evolution is witnessed today as states, organised crime groups, and private hackers are using sophisticated techniques by destabilising and disrupting critical architectures, particularly in the oil and gas industries. In this case, smaller states have turned into cyber fortresses mimicking Israel, Iran, and the US to gear up their cyber capabilities.[42] It has been noted that the Cyber Threat Intelligence (CTI) market will soar to $31 billion by 2030.[43] Adding to this, the Middle East average cost per data breach has surpassed $8.07 Million, way more than the global average of

$4.45 Million, while being second to the United States.[44] This indicates that cyber warfare has changed the battleground by remolding alliances and strategic interests of states. Moreover, it has allowed the simmering rivalries to fester into something catastrophic and deadly, thus suctioning global powers into their depth. Therefore, a cyber-pandemic is on the horizon, which will not only complicate attribution capabilities but will make offensive cyber warfare a tool of first resort.

Conclusion

Critical analysis of Iran's posture as a victim or aggressor indicates that increased western cyber assault has coerced Iran to strengthen its cyber capabilities. This is evident through its cyber infrastructure and technological collaboration with states like Russia and China. But, Iran's victimhood still persists due to low cyber protection and defense capabilities concerning foes, i.e., the US and Israel. Despite, Iran's countermeasures and development in cyber warfare, it still faces challenges concerning technological limitations, attribution difficulties, and response strategies. There is a huge gap between Iran (and allies, i.e., Russia and China) and technologically advanced states such as the US and Israel which possess both traditional and non-traditional security prowess. Moreover, Iran unlike its opponents is faced with domestic and international legitimacy dilemmas which have frequently diverted its attention. Coupled with this, Israel and the US have also unified to prevent Iran from enriching uranium beyond the permissible level, which has added further tensions to its volatile security outlook. In conclusion, Iran has been defending against a multi-front assault in the domain of cyber warfare which has significantly impacted its survival in international relations.

Notes and References

[1] Washington Free Beacon, "Iran, Russia Working Together to Launch Cyber Attacks, Former Lawmaker Claims," *Fox News*, 4 March 2014, https://www.foxnews.com/politics/iran-russia-working-together-to-launch-cyber-attacks-former-lawmaker-claims.

[2] Giacomo Spadoni, "IRGC Cyber-Warfare Capabilities," n.d., https://ict.org.il/UserFiles/IRGC%20Cyber-Warfare%20Capabilities.pdf.

[3] "Iranian Offensive Cyber Attack Capabilities Threat Evolution," 2020, https://sgp.fas.org/crs/mideast/IF11406.pdf.

[4] "Iranian Cyber Warfare," 2021, https://top-center.org/js/ckfinder/userfiles/files/Iranian%20Cyber%20Warfare_TopchubashovCenter.pdf.

[5] Krystal Bermudez, "The Islamic Republic's Internal Messaging Chaos," *FDD,* 19 April 2024, https://www.fdd.org/analysis/2024/04/19/the-islamic-republics-internal-messaging-chaos/.

[6] Marie Baezner, "Hotspot Analysis: Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions CSS CYBER DEFENSE PROJECT," May 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf.

[7] Giacomo Spadoni, "IRGC Cyber-Warfare Capabilities," n.d., https://ict.org.il/UserFiles/IRGC%20Cyber-Warfare%20Capabilities.pdf.

[8] Ibid.

[9] Ibid.

[10] "Israel-Iran Cyber War, Gas Station Attack," *The Iran Primer*, 2 November 2021, https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack.

[11] "History of Iranian Cyber Attacks and Incidents," *UANI*, 2024, https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents.

[12] "Israel Saw 43% Surge in Cyber Attacks from Iran, Hezbollah in 2023," *Iran International*, 3 April 2024, https://www.iranintl.com/en/202404036366.

[13] Jason Blessing, "The Growing Threat of Cyber Cooperation between Russia and Iran," *The Dispatch*, May 16, 2023, https://thedispatch.com/article/the-growing-threat-of-cyber-cooperation-between-russia-and-iran/.

[14] Ibid.

[15] Emilio Iasiello, "What Happens If China, Iran, and Russia Form a Cyber Tripartite?," *OODA Loop*, 3 May 2023, https://www.oodaloop.com/archive/2023/05/03/what-happens-if-china-iran-and-russia-form-a-cyber-tripartite/.

[16] "Russia Is Advantageous for Iran's Cyber Security - Lawmaker," *Iran International*, 2024, https://www.iranintl.com/en/202401010368.

[17] Ibid.

[18] Jason Blessing, "The Growing Threat of Cyber Cooperation between Russia and Iran," *The Dispatch*, 16 May 2023), https://thedispatch.com/article/the-growing-threat-of-cyber-cooperation-between-russia-and-iran/.

[19] Ibid.

[20] Emilio Iasiello, "What Happens If China, Iran, and Russia Form a Cyber Tripartite?," *OODA Loop*, 3 May 2023, https://www.oodaloop.com/archive/2023/05/03/what-happens-if-china-iran-and-russia-form-a-cyber-tripartite/.

[21] Eleni Kapsokoli, "Iran's Digital Authoritarianism as the Blueprint for National Sovereignty," *European Conference on Cyber Warfare and Security* 23, no. 1 (June 21, 2024): 233–40, https://doi.org/10.34190/eccws.23.1.2297.

[22] Ibid.

[23] "Russia Is Advantageous for Iran's Cyber Security - Lawmaker," *Iran International*, 2024, https://www.iranintl.com/en/202401010368.

[24] "Israel-Iran Cyber War, Gas Station Attack," *The Iran Primer*, 2 November 2021, https://iranprimer.usip.org/blog/2021/nov/02/israel-iran-cyber-war-gas-station-attack.

[25] Ibid.

[26] Ibid

[27] Reza Solgi, Hassan Khodaverdi, and Zohreh Poustinchi, "Pathology of the New Cyber Terrorism Threat to Iran's National Security," *International Journal of Political Science* 12, no. 1 (2022): 55–70, https://journals.iau.ir/article_694509_c5cf98073adb73c2b9f1bc4512369b21.pdf.

[28] Marie Baezner, "Hotspot Analysis: Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions CSS CYBER DEFENSE PROJECT," May 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf.

[29] Ibid.

[30] Ibid.

[31] Matthias Schulze, Josephine Kerscher, and Paul Bochtler, n.d., https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Schulze_December20_Cyber_Escalation_Research_01.pdf.

[32] "What the Defense Department's Cyber Strategy Says about Cyber Conflict," *Default*, 2023, https://www.lawfaremedia.org/article/what-the-defense-department-s-cyber-strategy-says-about-cyber-conflict.

[33] Matthias Schulze, Josephine Kerscher, and Paul Bochtler, n.d., https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Schulze_December20_Cyber_Escalation_Research_01.pdf.

[34] Middle East Policy, "Cyber Capabilities: Israel vs. Iran - Middle East Policy Council," *Middle East Policy Council*, August 24, 2021, https://mepc.org/commentaries/cyber-capabilities-israel-vs-iran/.

[35] Retired Major General Ahmed bin Ali al-Maymouni, "Specialized Studies," October 2020, https://rasanah-iiis.org/english/wp-content/uploads/sites/2/2021/04/THE-ACTIVE-FRONT-THE-CONSEQUENCES-OF-CYBERWARFARE-BETWEEN-IRAN-AND-ISRAEL.pdf.

[36] Marie Baezner, "Hotspot Analysis: Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions CSS CYBER DEFENSE PROJECT," May 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20190507_MB_HS_IRN%20V1_rev.pdf.

[37] Middle East Policy, "Cyber Capabilities: Israel vs. Iran - Middle East Policy Council," *Middle East Policy Council*, August 24, 2021, https://mepc.org/commentaries/cyber-capabilities-israel-vs-iran/.

[38] "How Israel's Pegasus Spyware Stoked the Surveillance Debate," *Council on Foreign Relations*, 2022, https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.

[39] Ibid.

[40] Natalia Krapiva, "What Spy Firm Cellebrite Can't Hide from Investors," *Access Now*, 26 May 2021, https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/.

[41] "Cyber Capabilities: Israel vs. Iran," *Middle East Policy Council*, 24 August 2021, https://mepc.org/commentaries/cyber-capabilities-israel-vs-iran/.

[42] Patrick McAteer, "Rising Cyber Threats in the Middle East – a Virtual Battleground," *Security HQ*, 29 November 2023, https://www.securityhq.com/blog/rising-cyber-threats-in-the-middle-east-a-virtual-battleground/.

[43] Ibid.

[44] Ibid.