Zoltán Prantner

IRAN AS AN EMERGING "CYBER POWER"?

ABSTRACT: *Iran is continuously developing its cyber capabilities to carry out increasingly sophisticated attacks against its regional and global adversaries, and to suppress certain social and political activities. Enforcers with varying levels of sophistication, acting on behalf of the Iranian Islamic Revolutionary Guard Corps, are engaged in a wide range of offensive cyber activities, including website content alteration, spear phishing, distributed denial of service attacks, theft of personally identifiable information or, in worse cases, the use of destructive malware, social media influence operations, and cyber-attacks with potential physical consequences against critical infrastructure.*

KEYWORDS: *Iran, United States of America, Gulf States, Stuxnet, cyber activity*

ABOUT THE AUTHOR:
Dr Zoltán Prantner is an associate professor of the Faculty of International Studies at the Kodolányi János University, Budapest, Hungary

INTRODUCTION

Hybrid warfare includes direct armed confrontation, cyber operations, disinformation campaigns and the spread of fake news. In this regard, it can be observed that Iran is currently striving for cyber dominance not only in the MENA region, but also worldwide. This is evidenced, inter alia, by the well-documented and varying success of Tehran's cyber-attacks against public and private sector assets to monitor or sabotage them in order to reduce the political and military power of rival states, or the dissemination of pro-Iranian messages and the telling of the 'Iran story' in an attempt to portray a more positive image of the country. The effectiveness of these efforts, however, has so far been severely limited by US economic sanctions and the recently expired UN arms embargo. As a result, Iran has essentially adopted what could be described as a 'soft war' strategy, using less regulated and non-kinetic means to achieve its goals abroad by sustaining low-level conflicts over the long term. In this respect, it sees its cyber programme as a means of asymmetric but proportionate retaliation against its political opponents. In addition, an analysis of Iran's ambitions shows that, while constantly promoting and promoting its revolutionary cause, it is constantly seeking to adapt its goals and capabilities to changes in the international environment and the new challenges it faces.

THE BACKGROUND OF IRANIAN CYBER CAPACITY

The strategy and development of Iran's cyber operations programme, launched in 2009, have been most influenced by the often state-sponsored cyber operations against the regime. In this regard, the Green Revolution of 2009, which Iranian officials simply described as an ‘insurgency’, the joint US-Israeli Stuxnet[1] attack on the Natanz nuclear facility in 2010, the Duqu[2] malware identified in 2011, and the Flame[3] malware detected in 2012 were the most significant, revealing the system’s vulnerabilities while allowing it to present itself as a victim. It also provided an incentive for Tehran to develop its domestic cyber capabilities in the background in an explosive way. In this respect, the establishment of the Supreme Council for Cyberspace in March 2012, following Ali Khamenei’s decree on the subject, was a fundamental change.[4] The new body was tasked with developing a strategy and blueprint for controlling domestic information as well as intelligence abroad. A rather sophisticated bureaucracy has been created to realise the stated goals, while the country’s overall cyber budget has more than tripled in five years.[5]

Despite the increased support, international experts say Tehran is still considered a third-tier cyber power in terms of the sophistication of its hackers, significantly below their more

[1] A malware spreading on Microsoft operating systems, specifically designed to target industrial process control systems. It is only triggered by the detection of the presence of specific high-speed motors and frequency converters used exclusively in Iranian uranium enrichment plants. It has destroyed at least 1000 nuclear centrifuges at Natanz, which is believed to have set back Iran’s nuclear programme by about two years. Warrick, J. “Iran’s Natanz nuclear facility recovered quickly from Stuxnet cyberattack”. Washington Post, 16 February 2011. https://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html?tid=a_inl_manual, Accessed on 3 February 2022.

[2] There is no reliable information about the Duqu’s creators and the exact purpose of the series of attacks. The targets identified suggest that Duqu was used to obtain information in an industrial control system environment. Due to its modular design, it could be capable of any specific task, but its components identified so far did not contain any direct malicious programming modules, such as the PLC reprogramming component in the case of Stuxnet. Zetter, K. “Son of Stuxnet Found in the Wild on Systems in Europe”. Wired, 10 October 2011. https://www.wired.com/2011/10/son-of-stuxnet-in-the-wild/, Accessed on 27 January 2022.

[3] Flame was identified by cybersecurity and antivirus firm Kaspersky in 2012. The malware, which was believed to have been present on Iranian computer networks for two years at the time, was capable of both extracting and deleting information (e.g. documents, social media conversations or keystrokes) from hacked devices. Zetter, K. “Meet ‘Flame,’ The Massive Spy Malware Infiltrating Iranian Computers”. Wired, 28 May 2012. https://www.wired.com/2012/05/flame/, Accessed on 27 January 2022.

[4] The panel included the president, cabinet ministers, the head of the Islamic Republic of Iran’s Broadcasting Service, the commander of the Iranian Republican Guard, and other senior officials from the intelligence and state security agencies. The Council’s membership was reorganised in 2015, resulting in an increase in the number of ministers sitting on it. The board is accountable only to the supreme leader and cannot be held to account by parliament. Fassihi, F. “Iran’s Censors Tighten Grip”. The Wall Street Journal, 16 March 2012. https://www.wsj.com/articles/SB10001424052702303717304577279381130395906, Accessed on 3 February 2022.

[5] Iran’s total cyber budget was around $76 million before 2011. Tehran claims that this amount has been increased to around $1 billion per year by 2016. Another striking figure is that the cybersecurity budget of the Ministry of Information and Communication Technology increased more than tenfold (from 42,073 million Iranian rials to 550,000 million) between 2013/2014 and 2015/2016. Finally, the budget for information technology infrastructure was increased by 20% following the nuclear agreement. “Iranian Internet Infrastructure and Policy Report Special Edition: The Rouhani Review (2013–15)”. Small Media, February 2015, 7. https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf, Accessed on 3 February 2022; Jones, S. “Cyber warfare: Iran opens a new front”. Financial Times, 26 April 2016. https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3, Accessed on 3 February 2022; Shafa, E. Iran’s Emergence as a Cyber Power. Strategic Studies Institute, 20 August 2014. http://ssi.armywarcollege.edu/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20, Accessed on 3 February 2022.

prestigious counterparts in China and Russia. The main reasons for this are international sanctions and a critical economic situation, which make it significantly more difficult for them to procure and develop high-end cybersecurity tools. They are weak on defence and rarely exploit zero-day vulnerabilities. At the same time, they make up for their lack of technical sophistication with social engineering tricks and by exploiting public vulnerabilities. They argue that this is why opportunistic Iranian APT (advanced persistent threat) groups are able to achieve success, especially against weak targets.[6]

THE EXECUTORS OF IRANIAN CYBER OPERATIONS

Following the Stuxnet attacks, the Iranian leadership attempted to set up a permanent, formal cyber organisation, but this proved to be a failure in a short time, as sanctions and insufficient technical support made it an insurmountable challenge to establish a reliable expert base. Although there were a number of suitable young candidates for the task, it was clear to the regime that they were motivated primarily by financial gain rather than political and religious vocation.[7] The response was therefore to develop a three-level approach with a network of individuals who were not formally affiliated with the government or the Iranian Revolutionary Guard Corps, but who were loyal to the regime and religiously committed.

Accordingly, the management and oversight of primary cyber operations fall under the purview of the Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security (Level 1). Their priorities are translated into segmented cyber tasks by their affiliated companies and front companies (Level 2), often outsourced directly to outsiders (Level 3). The process can thus be thought of as a kind of ‘government tendering’, whereby parties enter into a contractual agreement with each other to carry out part or all of a given target task, with payment only after the expected outcome has been achieved. The implementers therefore form a complex network of entrepreneurs, often competing with each other for contracts and greater government influence,[8] including individuals and groups as well as

[6] Warwick, M. “New report says China and Russia are not the cyber superpowers they are made out to be”. 29 June 2021. TelecomTV. https://www.telecomtv.com/content/security/new-report-says-china-and-russia-are-not-the-cyber-superpowers-as-they-are-made-out-to-be-41853/, Accessed on 26 January 2022.

[7] Apart from the potential bribery of candidates and the risk of recruitment by rogue intelligence services, another major problem, especially at the beginning, was that many of the talented Iranian hackers hated the system and lacked the discipline needed to work in government. Gundert, L. et al. “Iran’s Hacker Hierarchy Exposed. How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations”. Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf, Accessed on 3 February 2022.

[8] According to the Insikt Group estimates, more than 50 organisations competed for Iranian government-funded cyber projects in 2019. It also pointed out that the latter were often collaborating with each other, as the government’s objectives can often only be achieved with the cooperation of two or more companies. Iran’s Cyberattacks Capabilities. King Faisal Center for Research and Islamic Studies, January 2020, 12.

private companies and domestic academic institutions.[9] They are thus not a homogeneous group and their capabilities cover a broad spectrum.

At the bottom of the executive ranking is the community of hackers and cybercriminals who are involved in politically motivated disruptive operations. They mainly seek to obtain user credentials to gain access to computer networks, which they usually try to obtain through large-scale, low-skilled, less sophisticated spear phishing attacks. However, there has been an improvement in this area in terms of spear phishing efforts and a much more sophisticated use of so-called Denial of Service (DoS) attacks[10] against Iran's adversaries in the Middle East. At the intermediate level, there are already operators who, following a predictable pattern of tactics, techniques, and procedures (TTPs), typically target the community network, primarily to monitor the Iranian diaspora and internal opposition groups. At the top are those who specifically seek to develop unique malicious programs and use more advanced techniques to threaten their targets, such as DNA hijacking or more familiar web exploits.[11] The Iranian cyber workforce, on the other hand, includes not only those who organise and carry out attacks, but also those who evaluate the information they obtain. The latter are often mid- and top-level contractors in the hierarchy outlined above, as the diversity of targets means that they have the expertise and technical background necessary to analyse information illegally obtained from various sources.

The specific perpetrators of the Iranian attacks have consistently sought to preserve their anonymity to avoid retaliation, and have therefore diversified their TTPs over time to mask their activity and avoid being traced. The latter has been achieved by creating fictitious groups, using publicly available malware, moving them between companies, sharing their software, code fragments, and attack infrastructure, and engaging and increasingly activating various proxy groups and organisations allied with Iran as the armed conflicts in the Middle East escalated. The latter often benefit from Tehran's material and technical support and operate under the supervision of the Islamic Revolutionary Guard Corps. In exchange for ideological conviction and assistance from the Persian state, they often take responsibility for actions against Iran's rivals, thus enabling Tehran to avoid international

[9] Iranian higher education institutions can both provide the system with a way to discover talented young people and be an active participant in Iranian cyber activity. In this respect, Shahid Beheshti University, which has a specialised cyber research institute, and Imam Hossein University, founded by the Islamic Revolutionary Guard Corps, have become particularly famous. The latter has even been sanctioned by the US government for supporting Islamic Revolutionary Guard Corps operations. And a prime example of recruitment at universities is the case of Ayatollah Ali Khamenei, who in a speech to the university youth in 2014 asked his audience to prepare for cyber warfare. "Iran's Supreme Leader Tells Students to Prepare for Cyber War". Russia Today, February 13, 2014. https://www.rt.com/news/iran-israel-cyber-war-899/, Accessed on 29 January 2022.

[10] Denial of Service (DoS) attacks are designed to overload information systems, services or network resources to the point where they become unavailable or unable to perform their intended functions for their intended users. The objective is usually achieved by flooding the targeted machine or resource with unnecessary requests to overload it with artificially increased traffic and prevent legitimate requests from being fulfilled. The effectiveness of this type of attack is significantly increased when carried out by more complex, interconnected systems from multiple locations at the same time, known as a distributed denial of service (DDoS) attack. The use of this method was particularly popular among Iranian hackers in 2011–2013. Mezei K. "A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon". Pro Futuro, 8(1), 2018, 66–67. https://doi.org/10.26521/Profuturo/2018/1/4674

[11] Leyden, J. "Iranian cyber-threat groups make up for lack of technical sophistication with social engineering trickery". The Daily Swing, 1 July 2021. https://portswigger.net/daily-swig/iranian-cyber-threat-groups-make-up-for-lack-of-technical-sophistication-with-social-engineering-trickery, Accessed on 25 January 2022.

condemnation. However, in some cases, the Iranian state has made little effort to conceal its involvement, mainly in actions against civil and financial sector actors, essentially for propaganda purposes. In fact, it has been able to demonstrate both the vulnerability of the rival state and its own cyber capabilities and assertiveness vis-à-vis its global adversaries through the cases that have been brought to light.

TARGETS AND MOTIVES FOR CYBER OPERATIONS

As the background base has developed, expanded and evolved, the motives and targets of Iranian cyber operations have diversified. Reasons for deployment have included the intention of regional power projection, to monitor the regime's political opponents and symbolically attack its historical adversaries (notably the United States, Saudi Arabia,[12] the United Arab Emirates[13] and Israel), to retaliate against sanctions imposed by the international community, to support the growth of key domestic industries, and to steal unpublished research and intellectual property[14] from universities and academic institutions.[15] Accordingly, the targets of the attacks have been mainly government and military facilities, transport and travel companies, telecommunications operators and other critical national infrastructure, key industrial facilities in the Middle East region's economy (such as Saudi Aramco or Qatar's RasGas oil companies), dissidents, scientists, academic and scientific institutions, and defence companies. When all these targets are compared with the types of cyber-attacks commonly used, it can be said that the theft of Internet Protocol (IP) addresses and information mainly affects governments, manufacturers, academia, and dissidents. The wider support for access is mostly seen in the case of telecom operators and travel com-

[12] According to a survey, 95% of Saudi businesses experienced a cyber-threat to their operations in 2019. 85% of respondents reported a dramatic increase in the number of attacks affecting their business between 2017 and 2019 that severely affected both business operations (e.g. customer and employee data loss, ransomware payouts, theft and other financial losses) and operational technology. Tashkandi, H. "Cyberattacks hit 95% of Saudi businesses last year, says study". Arab News, 12 August 2020. https://www.arabnews.com/node/1718596/saudi-arabia, Accessed on 27 January 2022.

[13] According to the United Arab Emirates' cybersecurity chief, there was a 250% increase in the number of cyberattacks targeting the Gulf state in 2020, following the normalisation of relations with Israel. "Cyberattacks in UAE up 250% during pandemic, Emirati cyber chief says". Al-Monitor, 7 December 2020. https://www.al-monitor.com/originals/2020/12/cyber-attacks-uae-israel-kuwaiti-pandemic-whatsapp.html, Accessed on 27 January 2022.

[14] The US Department of Justice, for example, blamed the Mabna Institute, a subsidiary of the Islamic Revolutionary Guard Corps, for a targeted spear phishing campaign targeting 144 US and 176 other higher education institutions and more than 100,000 professors' email accounts worldwide between 2013 and 2017. The actions resulted in the illegal access of some 31.5 terabytes of scientific data worth a total of $3.4 billion from US universities alone, which was then used to upgrade Iran's infrastructure and technology or sold to domestic users. Hochberg, L. "Iran's cyber future". MEI@75, 23 February 2021. https://www.mei.edu/publications/irans-cyber-future, Accessed on 27 January 2022; Publicly Reported Iranian Cyber Actions in 2019. https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019, Accessed on 26 January 2022; US FBI. Iranian Mabna Hackers. https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers, Accessed on 27 January 2022.

[15] Parsons, E. and Michael, G. "Understanding the Cyber Threat from Iran". F-Secure, April 2019. https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran, Accessed on 26 January 2022.

panies. Finally, the intent to cause harm was most evident in the petrochemical industry and, in some cases, in government targets.[16]

The development of cyber capabilities is closely linked to Iran's nuclear programme at several points. By developing a nuclear weapon, Tehran would have gained a hegemonic position in the region and increased its support among the domestic public, while deterring rivals. With all this theoretically nullified by international sanctions and the nuclear deal, the Iranian state leadership began to use its cyber capabilities as an alternative means to achieve its original objectives and to avenge the restrictions imposed by the international community, especially after the US withdrawal from the Joint Comprehensive Plan of Action.

IRANIAN CYBER ACTIONS

Following the formation of the Supreme Council for Cyberspace, Iran carried out a number of cyber operations around the world over the past ten years, most of which have targeted PCs. All of these attacks were motivated by two main, not necessarily mutually exclusive, reasons. The first and more pronounced effort was primarily aimed at intelligence gathering and discreetly targeting a particular system with targeted and systematically developed malicious software, while not seeking to affect the operation of the facility. The detailed information collected and systematised was clearly intended to be used as power projection against targets following an adverse turn in diplomatic relations.[17] This was illustrated by the global cyber detection and infiltration campaign (Operation Clever[18]) conducted by Iran on a global scale between 2012 and 2014, or the intrusion into the flood protection system of the Bowman Avenue Dam in Rye Brook, New York, in August and September 2013.[19] The second, less dominant reason in terms of its proportions, was the launch of retaliatory attacks using rapid, sloppily planned and less sophisticated methods, which could be seen as a certain response to attacks on specific Iranian interests and facilities. Accordingly, Iranian hackers were involved in DDoS attacks against a number of major US financial firms and banks (Operation Ababil) from December 2011 to May 2013 in retaliation for the financial sanctions imposed by the Obama administration.[20] In addition, proxies linked to the Iranian regime used destructive malware to strike the Sands Casino in Las Vegas in

[16] Iran's Cyberattacks Capabilities … 15.

[17] Brennan, D. "U.S. Expects Iranian Cyber Attacks in Retaliation to New Sanctions, Experts Say". Newsweek, 8 August 2018. https://www.newsweek.com/us-expects-iranian-cyber-attacks-retaliation-new-sanctions-experts-say-1062977, Accessed on 26 January 2022.

[18] According to research by Cylance Inc., the Iranian cyber operation affected more than 50 entities in 16 countries, including the United States, Israel, China, Saudi Arabia, India, Germany, France and the United Kingdom. Cylance. Operation Clever. https://www.aclu.org/sites/default/files/field_document/Cylance-Operation-Cleaver-Report-1748-1833.pdf, Accessed on 3 February 2022.

[19] "Iranian hackers 'targeted' New York dam". BBC, 21 December 2015. https://www.bbc.com/news/technology-35151492, Accessed on 26 January 2022.

[20] During the above-mentioned period, approximately 46 U.S. financial institutions suffered DDoS attacks for a total of at least 176 days, for which the seven-member Iranian Izz ad-Din al-Qassam Cyber Fighters Group claimed responsibility in the most intense phase. Chabrow, E. "7 Iranians Indicted for DDoS Attacks against U.S. Banks". Bankinfo Security, 24 March 2016. https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989, Accessed on 26 January 2022.

2014 due to the owner's public anti-Iranian statements,[21] while cyber-attacks against Saudi Aramco and RasGas in Qatar were intended to avenge a cyber-attack on an Iranian oil facility in 2012. Iran has also initiated cyber-attacks to protect or support its allies in the region, such as the DDoS attack on Israel Defence Forces infrastructure during the 2014 Israeli-Palestinian conflict.[22]

Since 2016, with the outbreak of the current Saudi-Iranian proxy war, there has been a shift in emphasis in Iran's cyber strategy from intelligence gathering to initiating and executing sophisticated attacks that have caused immediate damage. This was demonstrated, inter alia, by the repeated use of Shamoon, a reverse-designed version of Stuxnet, against a number of Saudi government agencies, oil organisations and ministries.[23] The devastating virus rendered thousands of workstations unusable by destroying hard drives, deleting data, overwriting files, and making computers unavailable for power-up.[24] The attacks were followed by a lack of retaliatory response of similar intensity from rivals, providing an incentive for Tehran not only to continue its cyber operations but also to intensify them.

A year later, an advanced version of the virus targeted the Italian oil company Saipem and caused hundreds of corporate servers and personal computers to crash in the United Arab Emirates, Saudi Arabia, Scotland, and India. A similar action was carried out against Bapco, Bahrain's national oil company in 2019, a series of attacks hit the water infrastructure in Israel in 2020, and Iranian cyber spy groups targeted the 2018 mid-term elections and the 2020 presidential election in the United States. For example, a federal grand jury in New York indicted two Iranian nationals on 16th November 2021 for cyber-based disinformation activities. Among other things, they were charged with illegal obtaining data on more than 100,000 voters. They also sent threatening letters to tens of thousands of Democratic voters on behalf of the far-right Proud Boys in support of Donald Trump's presidential campaign, and disseminated disinformation about alleged vulnerabilities in election infrastructure.[25]

In addition to the attacks abroad, Tehran is also using its cyber capabilities to monitor and contain domestic discontent. Internet access has been cut off for the majority of the population following the killing of hundreds of protesters and bystanders by Iranian security forces over five days in November 2019 during a series of protests over a major fuel price hike.

[21] Sheldon Gary Adelson, founder, chairman and CEO of Las Vegas Sands Corporation, publicly proposed in the fall of 2013 that the United States strike Iran with a nuclear weapon. Pagliery, J. "Iran hacked an American casino, U.S. says". CNN Business, 27 February 2015. https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html, Accessed on 26 January 2022; Shwayder, M. "Adelson: US should drop atomic bomb on Iran". The Jerusalem Post, 24 October 2013. https://www.jpost.com/Diplomacy-and-Politics/Adelson-US-should-drop-atomic-bomb-on-Iran-329641, Accessed on 3 February 2022.

[22] Defense Intelligence Agency. Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance. August 2019, 36. https://www.iranwatch.org/sites/default/files/iran_military_power_v13b_lr.pdf, Accessed on 2 February 2022.

[23] Iran has used Shamoon to attack targets on at least three occasions, with Shamoon 1 causing the most damage, as the protection developed against the malware has significantly reduced the effectiveness of later versions. Deployments of later versions have therefore focused primarily on less prepared targets and on more vulnerable supply chains to key targets. Iran's Cyberattacks Capabilities … 15–16.

[24] Ms. Smith. "Saudi Arabia again hit with disk-wiping malware Shamoon 2". CSO, 24 January 2017. https://www.csoonline.com/article/3161146/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html, Accessed on 26 January 2022.

[25] Mangan, D. and Breuninger, K. "Two Iranians charged with spreading election disinformation, threatening people to vote for Trump". CNBC, 18 November 2021. https://www.cnbc.com/2021/11/18/two-iranians-charged-by-feds-in-election-interference-to-aid-trump-.html, Accessed on 4 February 2022.

A similar action was taken in February 2021, when internet bandwidth was restricted after days of bloody protests erupted in Baluchistan province following the killing of fuel traders. These drastic measures were accompanied by continued restrictions on digital rights and internet freedom, a clear reaction by the regime to the increasing activity of opposition protest organisers in the digital space. It also regularly infiltrates the websites and email accounts of political dissidents using open source research, and regularly censors their communications and the online content they share. This is complemented by an aggressive and effective disinformation campaign, using social pseudo-media accounts to share and promote false information to influence public opinion, reduce social tensions and create a positive image of the country.

In addition to political opponents and internal opposition groups, the surveillance of the Iranian diaspora is also a continuing priority for the Iranian regime's cyber operations. In this case, the specific individuals are mainly targeted through spear phishing attacks and SMS messages to induce them to open malicious links or attachments. For example, in February 2021, the Dutch public broadcaster Dutch Public Service Broadcasting reported that the Iranian regime used a Dutch server linked to an Iranian base to collect data on dissidents in the Iranian diaspora.

OUTLOOK

The new US foreign policy towards Iran, i.e. to seek a diplomatic solution and negotiate, raises the possibility that Tehran's hostile relationship with the international community could be normalised. However, even if the latter were to happen, it may not significantly reduce the cyber threat posed by Iran. This is evidenced, inter alia, by the fact that the Iranian Revolutionary Guard Corps is currently lobbying for a parliamentary rewrite of laws governing internet use to improve state control and further increase the effectiveness of intelligence capabilities. Its aim is clearly to establish a national intranet and disconnect Iran from the global internet network. To this end, regime-backed front companies have already produced spyware-enabled mobile apps and VPNs, several of which are already available on the global mobile app market.[26] In addition, it is almost certain that the improvement of Shamoon continues, which Iran will presumably use against its adversaries.

Finally, there is the closer cooperation with China, declared in 2019, and the cybersecurity cooperation agreement signed with Russia on 26th January 2021. Although these agreements are formally aimed at improving information technology and closing defence gaps, they nevertheless increase the challenge for Iran's rivals in the region and provide an opportunity for the transfer of foreign technology to Iranian proxy organisations operating in the region.[27] This being said, even as relations with Tehran improve, it will be of paramount

[26] Piroti, M. "The Ever-Growing Iranian Cyber Threat". BESA Centre Perspectives Paper, No. 2.160, 26 September 2021. https://besacenter.org/iran-cyber-threat/, Accessed on 25 January 2022.

[27] Doffman, Z. "Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S.". Forbes, 6 July 2019. https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/?sh=7a4fba5f42eb, Accessed on 27 January 2022. El-Masry, A. "The Abraham Accords and their cyber implications: How Iran is unifying the region's cyberspace". MEI@75, 9 June 2021. https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace, Accessed on 27 January 2022.

importance to continuously monitor the development of Iran's cyber capabilities, identify the challenges they pose and develop effective cyber defence policies to address them.

BIBLIOGRAPHY

- Brennan, D. "U.S. Expects Iranian Cyber Attacks in Retaliation to New Sanctions, Experts Say". *Newsweek,* 8 August 2018. https://www.newsweek.com/us-expects-iranian-cyber-attacks-retaliation-new-sanctions-experts-say-1062977, Accessed on 26 January 2022.
- Chabrow, E. "7 Iranians Indicted for DDoS Attacks against U.S. Banks". *Bankinfo Security,* 24 March 2016. https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989, Accessed on 26 January 2022.
- "Cyberattacks in UAE up 250% during pandemic, Emirati cyber chief says". *Al-Monitor,* 7 December 2020. https://www.al-monitor.com/originals/2020/12/cyber-attacks-uae-israel-kuwaiti-pandemic-whatsapp.html, Accessed on 27 January 2022.
- Cylance. *Operation Clever*. https://www.aclu.org/sites/default/files/field_document/Cylance-Operation-Cleaver-Report-1748-1833.pdf, Accessed on 3 February 2022.
- Defense Intelligence Agency. *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance*. August 2019. https://www.iranwatch.org/sites/default/files/iran_military_power_v13b_lr.pdf, Accessed on 2 February 2022.
- Doffman, Z. "Cyber Warfare Threat Rises As Iran And China Agree 'United Front' Against U.S.". *Forbes,* 6 July 2019. https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/?sh=7a4fba5f42eb, Accessed on 27 January 2022.
- El-Masry, A. "The Abraham Accords and their cyber implications: How Iran is unifying the region's cyberspace". *MEI@75,* 9 June 2021. https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace, Accessed on 27 January 2022.
- Fassihi, F. "Iran's Censors Tighten Grip". *The Wall Street Journal,* 16 March 2012. https://www.wsj.com/articles/SB10001424052702303717304577279381130395906, Accessed on 3 February 2022.
- Gundert, L. et al. "Iran's Hacker Hierarchy Exposed. How the Islamic Republic of Iran Uses Contractors and Universities to Conduct Cyber Operations". *Recorded Future*. https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf, Accessed on 3 February 2022.
- Hochberg, L. "Iran's cyber future". *MEI@75,* 23 February 2021. https://www.mei.edu/publications/irans-cyber-future, Accessed on 27 January 2022.
- *Iran's Cyberattacks Capabilities*. King Faisal Center for Research and Islamic Studies, January 2020.
- "Iran's Supreme Leader Tells Students to Prepare for Cyber War". *Russia Today,* February 13, 2014. https://www.rt.com/news/iran-israel-cyber-war-899/, Accessed on 29 January 2022.
- "Iranian hackers 'targeted' New York dam". *BBC,* 21 December 2015. https://www.bbc.com/news/technology-35151492, Accessed on 26 January 2022.
- "Iranian Internet Infrastructure and Policy Report Special Edition: The Rouhani Review (2013–15)". *Small Media,* February 2015, 7. https://smallmedia.org.uk/sites/default/files/u8/IIIP_Feb15.pdf, Accessed on 3 February 2022.
- Jones, S. "Cyber warfare: Iran opens a new front". *Financial Times,* 26 April 2016. https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3, Accessed on 3 February 2022.

- Leyden, J. "Iranian cyber-threat groups make up for lack of technical sophistication with social engineering trickery". *The Daily Swing,* 1 July 2021. https://portswigger.net/daily-swig/iranian-cyber-threat-groups-make-up-for-lack-of-technical-sophistication-with-social-engineering-trickery, Accessed on 25 January 2022.
- Mangan, D. and Breuninger, K. "Two Iranians charged with spreading election disinformation, threatening people to vote for Trump". *CNBC,* 18 November 2021. https://www.cnbc.com/2021/11/18/two-iranians-charged-by-feds-in-election-interference-to-aid-trump-.html, Accessed on 4 February 2022.
- Mezei K. "A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon". *Pro Futuro,* 8(1), 2018, 66–83. https://doi.org/10.26521/Profuturo/2018/1/4674
- Ms. Smith. "Saudi Arabia again hit with disk-wiping malware Shamoon 2". *CSO,* 24 January 2017. https://www.csoonline.com/article/3161146/saudi-arabia-again-hit-with-disk-wiping-malware-shamoon-2.html, Accessed on 26 January 2022.
- Pagliery, J. "Iran hacked an American casino, U.S. says". *CNN Business,* 27 February 2015. https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html, Accessed on 26 January 2022.
- Parsons, E. and Michael, G. "Understanding the Cyber Threat from Iran". *F-Secure,* April 2019. https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran, Accessed on 26 January 2022.
- Piroti, M. "The Ever-Growing Iranian Cyber Threat". *BESA Center Perspectives Paper,* No. 2.160, 26 September 2021. https://besacenter.org/iran-cyber-threat/, Accessed on 25 January 2022.
- *Publicly Reported Iranian Cyber Actions in 2019*. https://www.csis.org/programs/technology-policy-program/publicly-reported-iranian-cyber-actions-2019, Accessed on 26 January 2022.
- Shafa, E. *Iran's Emergence as a Cyber Power*. Strategic Studies Institute, 20 August 2014. http://ssi.armywarcollege.edu/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20, Accessed on 3 February 2022.
- Shwayder, M. "Adelson: US should drop atomic bomb on Iran". *The Jerusalem Post,* 24 October 2013. https://www.jpost.com/Diplomacy-and-Politics/Adelson-US-should-drop-atomic-bomb-on-Iran-329641, Accessed on 3 February 2022.
- Tashkandi, H. "Cyberattacks hit 95% of Saudi businesses last year, says study". *Arab News,* 12 August 2020. https://www.arabnews.com/node/1718596/saudi-arabia, Accessed on 27 January 2022.
- US FBI. *Iranian Mabna Hackers*. https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers, Accessed on 27 January 2022.
- Warrick, J. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack". *Washington Post,* 16 February 2011. https://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html?tid=a_inl_manual, Accessed on 3 February 2022.
- Warwick, M. "New report says China and Russia are not the cyber superpowers they are made out to be". 29 June 2021. *TelecomTV*. https://www.telecomtv.com/content/security/new-report-says-china-and-russia-are-not-the-cyber-superpowers-as-they-are-made-out-to-be-41853/, Accessed on 26 January 2022.
- Zetter, K. "Son of Stuxnet Found in the Wild on Systems in Europe". *Wired,* 10 October 2011. https://www.wired.com/2011/10/son-of-stuxnet-in-the-wild/, Accessed on 27 January 2022.
- Zetter, K. "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers". *Wired,* 28 May 2012. https://www.wired.com/2012/05/flame/, Accessed on 27 January 2022.