TOP CHUBASHOV CENTER

SPECIAL REPORT

MAY 2021

IRANIAN CYBER WARFARE

About Topchubashov Center

The Topchubashov Center is an independent non-profit think tank based in Baku, Azerbaijan. It covers the spheres of international affairs, geopolitics, security and energy with the focus on Central and Eastern Europe, Caucasus, Central Asia and Middle East. The Center aims to establish the standards of high-quality impartial research and create an international network of authors sharing similar values and worldview.

1. Iranian hybrid warfare and cyber strategy

Iran is a rational actor and has a precise military strategy which is not only driven by its ideologies. The Iranian military strategy and the international context, explain the modus operandi and the choice of tools of warfare.

According to Abdolrasool Divsallar, the co-leader of the Regional Security Initiative at the Middle East Directions Programme, Iran is led by a cognitive context of strategic thinking.[1] This aggregated concept shapes the final Iranian military strategy. It gathers various driving forces such as its threat perception and interpretation of security threats in the world, the change of its national resources as well as sociological and historical background. According to this researcher, the main driver of the Iranian regional policy hinges on its threat perception of the Iranian elites which is rooted in a deep sense of insecurity regarding the sustainability of its regime as well as the fear to be attacked by Western and regional hostile forces.

The Iranian military strategy is led by the preservation of the regime and aims at repelling any contradicting influences.[2] The Iranian regime is thoroughly controlling its population to fend off the presence of its enemies near its borders to ensure the stability of Iran. Since the 1979 revolution, the Iranian regime is threatened by hostile powers near its borders (from Iraq, Israel or the Gulf countries). "As a revolutionary state, Iran constantly worries about potential instability and counter-revolution triggered by its adversaries during conflict," Andrew McInnis says.[3] These external threats overlap with internal opposition movements that are perceived as the consequence of the influence of Western values on the Iranian population. As the Ayatollah Khamenei emphasized in 2016, "the enemy is seeking to pervert devoted and righteous youths from the essence of religion; today this is being done across the cyber world."

These external threats overlap with internal opposition movements that are perceived as the consequence of the influence of Western values on the Iranian population.

The Iranian regime is also playing a zero-sum game policy on the international stage. "Tehran's doctrines reflect this porousness across the spectrum of offensive and defensive operations", reported Andrew McInnis.[4] To increase the security of its own country and regime, Iran considers that it needs to decrease the security of its main regional enemies. A position of regional hegemon would be perceived as stabilizing for the Iranian elite to secure the perennation of the regime to and protect it from any external interference.

[1] https://middleeastdirections.eu/event/irans-cognitive-context-of-strategic-thinking-presentation-by-abdolrasool-divsallar/
[2] https://www.iiss.org/blogs/analysis/2017/12/gulf-security
[3] https://www.iiss.org/blogs/analysis/2017/12/gulf-security
[4] https://www.iiss.org/blogs/analysis/2017/12/gulf-security

However, this threat perception is seen as very offensive from its regional enemies. Nevertheless, it should be highlighted that the Iranian threat perceptions of its security environment in the Middle East are not a blue-sky conception. The Iranian actions are very often the result of a long chain of attacks against its regime from the Gulf countries, the U.S., Iraq and Israel.[5] Its isolation on the international stage increased this negative perception and reduces the window of opportunity for possible negotiations. Very few reports exist on foreign attacks against the Iranian regime and most researchers concentrate mostly on the destabilizing actions of Iran in the Middle East without taking into consideration the whole security architecture in the region.

The Iranian actions intervene very often in a tit for tat style of confrontation occurring in a very tense context and under a great internal and external pressure.[6]

Iran is a rational actor calculating between its threat perception and the need to defend its territory and its available means to ensure these goals.

However, its international isolation and the lack of financial means hindered Iran to invest in sophisticated armed forces. To keep the deterrence balance positive, the Iranian regime relied on asymmetric means of warfare.

This strategy contrasts sharply with the current economic and military means available to the Gulf countries.[7] Military experts highlighted the current shift in the balance of power in the Middle East, advantaging the Gulf countries. In 2016, Saudi Arabia invested more than 113,722 billion dollars in its defense acquisition.[8] Usually, Gulf countries dedicate on average around 10% of their whole GDP to this sector while Iran can invest only 3% of its GDP.[9] Moreover, the current economic context in Iran is particularly gloom due to the current sanctions imposed against its regime by the U.S. as well as the coronavirus crisis lowering the global oil prices.[10]

Iran is a rational actor calculating between its threat perception and the need to defend its territory and its available means to ensure these goals.

Due to lack of economic resources and the need to ensure the security of its regime, Iran strives to avoid at all cost any confrontation against potential enemies but to demonstrate its determination to retaliate efficiently in case of a direct attack against its territory. This very delicate balance is epitomized in Iranian hybrid warfare.[11]

[5] https://www.limesonline.com/cartaceo/lodio-arabo-spinge-teheran-sullorlo-della-guerra?prv=true
[6] https://www.iiss.org/blogs/analysis/2017/12/gulf-security
[7] https://www.limesonline.com/cartaceo/lodio-arabo-spinge-teheran-sullorlo-della-guerra?prv=true
[8] https://www.limesonline.com/cartaceo/lodio-arabo-spinge-teheran-sullorlo-della-guerra?prv=true
[9] https://www.csis.org/analysis/gulf-and-irans-capabilities-asymmetric-warfare
[10] https://carnegieendowment.org/sada/83350
[11] https://www.trtworld.com/magazine/who-will-win-a-hybrid-war-between-the-us-and-iran-32817

According to the NATO website, "hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, and deployment of irregular armed groups and use of regular forces.[12] Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations."
The Iranian hybrid warfare is a specific way to address the Iranian asymmetric warfare which tries to impose a permanent sub-level of warfare which would be too low to foster a kinetic and direct retaliation from its enemies but with a sufficient level of violence to decrease the security of its regional counterparts.

According to Kelsey Atherton, a defense expert, "hybrid warfare is an attempt to acknowledge the holistic nature of actions taken by states in conflict, but instead of treating it as timeless and in the grey area of less-than-total-war, it rebrands it as a new phenomenon uniquely aided by modern technology."[13]

The goal for Iran is to keep the enemy in a state of confusion and a grey zone of warfare. The enemies would be denied the possibility to start the conflict unless to bear the responsibility of the total war and to be depicted as the aggressor. Iran can, therefore, keep its image of a martyr state which is a useful concept to frame its ideology and to use it for its internal politics.[14] Moreover, the use of hybrid tools of warfare impedes the enemy the possibility to win a decisive and visible victory which could be used politically afterwards.

The enemies would be denied the possibility to start the conflict unless to bear the responsibility of the total war and to be depicted as the aggressor.

Tehran uses very innovative means of warfare to implement these goals and impose pressure on all sensitive targets of its enemies.

The three tools that are mainly used by the Iranian regime to implement hybrid warfare are in the cyberspace, the use of proxies and a small part of its maritime strategy.

According to the UN Security Council Resolution 1113 (2011), "cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity." [15]

[12] https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=uk

[13] https://www.trtworld.com/magazine/who-will-win-a-hybrid-war-between-the-us-and-iran-32817
[14] https://www.iiss.org/blogs/analysis/2017/12/gulf-security
[15] https://books.google.fr/books/about/On_Cyberwarfare.html?id=jxvfrQEACAAJ&redir_esc=y

Cyberwarfare is a new type of danger that is emerging on the military battlefield. The increasing digitalization and urbanization raised the vulnerabilities of the economies to these new threats. Many States are developing these capabilities and the potential to hit any targets in the world, any time, at a minimal cost and maximum deniability.

Cyberspace is the perfect area of confrontation in hybrid warfare. It allows Iran to hit sensitive targets of the enemy, in the civilian and in the military spheres while it ensures the deniability of its actions. It is particularly difficult to retrace the responsibility of the Iranian government. The limits between military actions and fraudulent acts are blurred as well.

Cyber power could also improve Iranian soft power and have repercussions on the physical world. For Kueh, "cyber power is the ability to use the cyberspace to create advantages which influences the environment and hits the interconnectivity of all military elements: defense, diplomacy, informatics, and economics".

Cyberwarfare includes, therefore information warfare, espionage and also sabotages and can have a very large impact on physical infrastructures which are more and more digitalized.[16] Iran developed a large range of cyber tools with various degrees of violence implemented.

The Iranian cyber tools span from propaganda, disinformation campaigns, media manipulation, cyber-attacks, cyber theft, to a proxy cyber operation that can degenerate to overt conflict.

Iran uses information warfare in the Middle East through the influence of media and the support to cultural and diaspora to spread a positive image of the Iranian community in the world, and control its diaspora on cyberspace. However, the core of the Iranian cyber strategy relies on its hard-cyber operations (espionage and sabotage).

Iranian cyberwarfare was implemented since the 2010s with the emergence of the Green Movement, destabilizing the internal regime through the use of social media by demonstrators and with the discovery of Stuxnet, the first cyber weapon used against Iran. Iran started to develop its national technological means to control the use of the Internet by the population as well as offensive tools of warfare to attack its external enemies. These milestones were correlated with the huge development of messaging apps and web communication tools used in the Middle East and the emergence of the Arab Spring. The revolution against the power of Bashar Al Assad seriously threatened the Shia axis implemented by the Iranian regime connecting the Lebanese Hezbollah with Iraqi Shia militias. These popular waves of demonstrations were

Cyberwarfare includes, therefore information warfare, espionage and also sabotages and can have a very large impact on physical infrastructures which are more and more digitalized.

[16] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

construed as internal massive subversion launched by the West, as Russia considered that the Eastern coloured revolutions were fostered by Western actions.[17]

The first developments of the Internet in Iran were characterized by the increasing control of the Iranian government on the information space. Iran was one of the first countries in the Middle East of having benefitted from the Internet since 1993. The first Internet providers could sell their services widely to the Iranian population since 1995.[18] Very quickly, the Iranian government distrusted American Internet companies in operating on the global Internet and available in Iran. The Iranian government feared the potential hegemony of the West on the cyber space that could influence directly the Iranian population without any control possible for the government. The Iranian regime was very suspicious about the western-led development of the Internet which was presented as a tool to promote freedom and democratic values on the American side. For Iran, this development was perceived as contradicting its interests and a source of destabilization since the 1990s until nowadays. According to the IRGC Deputy Commander Hossein Salami, "we are in an atmosphere of a full-blown intelligence war with the U.S. and the front of enemies of the Revolution and the Islamic system.[19] This atmosphere is a combination of psychological warfare and cyber operation, military provocations, public diplomacy, and intimidation tactics."

The Iranian government started to implement committees and organizations to oversee the use of the Internet by the population. The Committees to regulate oversight of prohibited web resources was implemented in 2002 and put under the authority of the Ministry of Intelligence (MOI), the Ministry of Culture and Islamic orientation and the Ministry of Justice. In 2003, the government established the Supreme Council for Information Security to monitor the activities in the cyberspace.[20] In 2004, the Supreme Council for Science, Research and Technology was created to define the policies and plan to develop the actions of the Iranian state in the cyber field and in the information sphere. In July 2009, the Supreme Council of the Cultural Revolution set up the Committee to identify unauthorized sites.[21] This organization served to identify the prohibited websites (mainly pornography and political opponents' blogs) and "criminal content".

> The main watershed in the control of the Internet by the Iranian government operated with the Green Movement in 2009.

The main watershed in the control of the Internet by the Iranian government operated with the Green Movement in 2009.[22] These popular demonstrations were triggered after allegations from the political adversary (Mir Hossein Mousavi) against the then incumbent

[17] https://www.tandfonline.com/doi/full/10.1080/03932729.2019.1586147
[18] https://russiancouncil.ru/cyberiran

[19] https://en.isna.ir/news/98022915101/Iran-US-locked-in-serious-war-of-intelligence-IRGC-Commander
[20] https://russiancouncil.ru/cyberiran
[21] http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3
[22] https://www.washingtoninstitute.org/policy-analysis/irans-lengthening-cyber-shadow

president, stating that President Ahmanidejad falsified the results of the Iranian presidential elections. Most of protestors used available messaging apps and all tools available on the Internet to organize their demonstrations and spread criticism against the government. During this event, the Iranian government tried to infiltrate the accounts of the protesters and to block them.[23] All websites related to Mir Hossein Mousavi were blocked, and the government attempted to infiltrate messaging apps (such as Yahoo messenger, Messenger, and Google chat). The suspicion from the Iranian government increased when the first allegations from the Guardian confirmed that the American government demanded of the Twitter to provide its services to Iranian protesters to support the demonstrations.[24]

With the second mandate of President Ahmanidejad, access to the Internet was reduced for Iranian citizens. The Rouhani administration pursued the same policy with the development of filtering systems and censorship, and the limit of the speed of the Internet.[25] The Iranian government launched the development of a national Internet, separated from the global one.[26] The Iranian government increased its control of the Internet service providers as well as of telecommunication infrastructures, controlling the activities of the Iranians.
The development of the Iranian cyber warfare was correlated to the cyber-attacks targeted against Iran. The Iranian government started to develop its external offensive cyber program following the Stuxnet attack targeting its nuclear infrastructures in 2010.[27]

The Stuxnet attack, launched in the framework of the operation Olympic Games was reportedly a malware created in collaboration between the CIA and the Israeli intelligence services. It was considered as the very first massive cyber weapon ever created. The malware triggered the self-destruction of the Natanz enrichment centrifuges by targeting the supervisory control and data acquisition SCADA system, disrupting the working of the centrifuges. The two intelligence services allegedly collaborated to place implants in Iranian computers. This attack significantly delayed the creation of a nuclear bomb by the Iranian regime. The attack destroyed 1/5 of the Iranian nuclear centrifuges. During the same period, another virus was discovered, the Nitro Zeus in 2012.[28] Iran was the target of other cyber-attacks from the U.S. and regional adversaries. The Duqu and Flame malware were discovered in Iran in 2012 and targeted the Iranian Ministry of Oil and the National Oil Company. In 2012, the Iranian Central Bank, the Ministry of Culture as well as drilling platforms were targeted again.

[23] https://www.article19.org/ttn-iran-november-shutdown/
[24] https://www.nytimes.com/2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html?_r=0
[25] https://www.article19.org/ttn-iran-november-shutdown/

[26] https://opennet.net/research/profiles/iran
[27] https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[28] https://www.nytimes.com/2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html?_r=0

Iran dramatically increased its capabilities in cyber warfare over the past few years.[29] Since his first term of President Rouhani, the security budget of Iran has increased by 1,200% (according to a report from the British technology firm Small Media) in 2015. In 2019, the Iranian government invested 225 million dollars in the Iranian innovative funds to support IT companies and start-ups which are also fully part of the Iranian cyber ecosystem.[30] During the 8th National civil defence forum in Tehran in 2019, the head of the Iranian civilian defence organization, brigadier-general Gholamraza Jalali, proposed a new hybrid warfare definition based on the development of cyber capabilities. Although the Iranian cyber capabilities are not comparable with the very high level and sophisticated cyber arsenal present in Israel and the U.S., the Iranian hackers are particularly motivated and can inflict severe damages even through unsophisticated attacks.

In 2019, the Iranian government invested 225 million dollars in the Iranian innovative funds to support IT companies and start-ups which are also fully part of the Iranian cyber ecosystem.

In 2019, according to an edition of the Cyber week in Israel, Yigal Unna the director-general of the Israeli National Cyber Directorate stated that Iran was among the 5th most active cyber actors in the world.[31] The Iranian regime became particularly active in espionage against regional targets as well as sabotage and costly operations. Microsoft reported in a survey in March 2020 that Iranian cyber groups targeted more than 200 companies in the world between 2017 and 2019.[32]

2. Iranian cyber ecosystem

The Iranian government built its cyber strategy on the deniability and ambiguity of its actions.[33] To reach this goal, Iran developed a very complex cyber ecosystem to blur the links between it and various entities. According to experts, the Iranian hacking scene emerged from the 2000s and the state-aligned activities appeared from 2007. According to Collin Anderson, a researcher focused on cybersecurity and Karim Sadjapour, a senior fellow at the Carnegie Endowment for International Peace, the Iranian hackers hinge less on the sophistication of their actions than on their persistence, opportunism and on the enemies' vulnerabilities to succeed in their cyber warfare.[34]

[29] https://www.inss.org.il/publication/irans-activity-in-cyberspace-identifying-patterns-and-understanding-the-strategy/
[30] http://bit.ly/IranGov'tInvests_225m_in_Innovation_Fund
[31] https://www.inss.org.il/publication/irans-activity-in-cyberspace-identifying-patterns-and-understanding-the-strategy/
[32] https://www.wsj.com/articles/iranian-hackers-have-hit-hundreds-of-companies-in-past-two-years-11551906036
[33] https://www.washingtoninstitute.org/policy-analysis/irans-lengthening-cyber-shadow
[34] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

Two types of actors can be distinguished among the Iranian cyber ecosystem. They can be offensive or defensive. Their affiliation with the Iranian government and services cannot be proven despite some signs of collaboration between the various entities.

The highest state organization working in the design of the Iranian cyber warfare is the Iranian Supreme Council of Cyberspace which was created in 2012 by the Ayatollah Khamenei.[35] This organization is also known as the High Council of Cyberspace. According to the Congressional research services, this Council "coordinates cyberspace policy for the Iranian government and coordinates between offensive and defensive cyber operations".[36] It is reportedly made of senior officials such as the incumbent Iranian President, key Ministers, Chief Commander of the Islamic Revolution Guards Corps, Police Chief, the head of the Islamic Propagation Organization, the head of the state-run Radio and TV networks (IRIB), the chairman of parliament's Cultural Committee, and seven other members who are directly appointed by Ayatollah Ali Khamenei. The organization works allegedly under the orders of the government and the IRGC. Reporters Without Borders considered this body as among the twenty worst press freedom's digital predators in 2020.[37]

Other major State institutions participate in the design and the use of the Iranian cyber capabilities. The Iranian Ministry of Intelligence and Security (MOIS) is the organization that is specialized in signals intelligence and collecting information from electronic communications. The MOIS is the national intelligence service of Iran. The service allegedly tracks Iranian diaspora and monitor their activities on the cyber sphere. The Ministry of Information and Communication Technologies is also a key actor in the Iranian internal information warfare. The Ministry controls the national telecom sector and helps the government to control the activities of the Iranian population through telecommunications.

2.1. Defensive entities

The Iranian cyber defense is mostly assured and coordinated by the National Passive Defence Organization (NPDO). This organization was created in 2003 (in the wake of the operation Iraqi Freedom) and serves to coordinate all the Iranian defensive strategies and to improve the survivability of the Iranian military and civilian infrastructures. According to the Iranian law, the NPDO is in charge of "policymaking, planning, directing, organizing, coordinating, monitoring, and operating the passive defense and civil defense… activities of enforcement agencies."[38] This body is affiliated to the Iranian General Staff. It is led by brigadier-general in the Islamic Revolutionary Guard Corps Gholamreza Jalali Farahani since 2015.

[35] https://www.nligf.nl/v1/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf
[36] https://fas.org/sgp/crs/mideast/IF11406.pdf
[37] https://rsf.org/en/iran

[38] https://www.washingtoninstitute.org/policy-analysis/irans-passive-defense-organization-another-target-sanctions

This body was listed by the European Union on July 26, 2010, as an entity linked to Iran's proliferation-sensitive nuclear activities or Iran's development of nuclear weapon delivery systems. The organization is put directly under the authority of the Ayatollah.[39]

Regarding its role in the Iranian cyber ecosystem, the NPDO must protect the country from any cyber-attacks and cyber threats from inside and from outside. According to experts, the NPDO use "all national cyber and kinetic resources to deter, prevent, deny, identify, and effectively counter any cyberattack against… Iran's national infrastructure by either hostile foreign states or [domestic] groups supported by them." [40] The organization must therefore protect and ensure the resilience of the critical facilities and also to limit the freedom of speech of the Iranian political opponents.

> In 2011, the Cyber Defense Headquarters, also known as the Cyber Headquarters was created within the NPDO.

In 2011, the Cyber Defense Headquarters, also known as the Cyber Headquarters was created within the NPDO.[41] This organization overseas the Computer Emergency Response Team (CERT and MAHER) activities in cyber field deployed at the national level. The headquarters works in coordination with the Iranian Ministry of Information and Communication and the Council of the Cultural Revolution.

The Cyber Defense Command is also acting under the NPDO organization. The command may have been created as a corollary to the U.S. Cyber Command. It controls directly the Iranian cyber police or the Police for the Sphere of the Production and Exchange of Information (FATA in Persian).

The Iranian Cyber Police is a law enforcement unit. The Cyber Police is responsible for prosecuting what is considered as Internet crimes in Iran. This body tracks online activity within Iran, including infiltrating websites and email accounts of political dissidents. The Iranian Cyber Police first existed as a specific cell within the Iranian Police since 2009.[42] It was officially created in 2011. It controls users, infiltrates dissident websites and increases its control against the Iranian populations online and in cyber cafés.[43] The FATA collect all personal data on the users using computers in such cafés and retrace their researches and arrest them if their activities are suspicious.

[39] https://fas.org/sgp/crs/mideast/IF11406.pdf
[40] https://fas.org/sgp/crs/mideast/IF11406.pdf
[41] https://russiancouncil.ru/cyberiran

[42] http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3
[43] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134

2.2. Offensive actors

The Iranian Revolutionary Guard Corps (IRGC) is one of the main body regarding offensive cyber operations. The IRGC concentrates the best of the Iranian armed forces from intelligence, missile and naval programs.

According to the Cyber Sharafat, the idea of an Iranian cyber Army was first developed by the IRGC in 2005.[44] The National Council of Resistance of Iran (NCRI), an opposition movement based in France and Albania, referred that the IRGC have had a cyber force since 2008.[45] The Cyber Sharafat reported that this branch was initially called the cyber watchdog, and integrated as a branch of Tehran Mohammad Rasulullah Corps, including 3,000 forces.[46] According to this source, the IRGC hired at the beginning foreign hackers (allegedly from Russia and China) to train the Iranian technicians.

> Since 2009, the IRGC tracks political dissidents on the Internet and trains a wide range of hackers.

The IRGC allegedly includes a specific structure specialized in electronic warfare, named the Jangal organization.[47] According to some reports, this unit could include 2,400 operatives and is allocated a specific budget of 76 million dollars (separated from the one from the General Staff).[48] According to the Cyber Sharafat, would have 250,000 active members and 12,000 reserve members.[49] This source identified also Mansoor Amini, Mehdi Saremi and Mujtaba Ahmadi, as members of the management team of this unit.

Since 2009, the IRGC tracks political dissidents on the Internet and trains a wide range of hackers. After the 2009 revolution, these tasks were incorporated into the intelligence branch of the IRGC. This body recruits very highly skilled political workforce that can combine their adhesion to the values of the Iranian regime and their technical skills.[50] After the Green revolution, the IRGC particularly emphasized the indoctrination of its cyber forces and its population to avoid the development of digital skills among dissident groups. According to the NCRI, the IRGC cyber forces have their headquarter located at the Ammar base.[51] The IRGC cyber command is also decentralized and divided between the 31 Iranian provinces.[52] According to a document found by the Israeli cybersecurity company Clear Sky, the IRGC

[44] https://cybershafarat.com/2019/03/10/cyber-war-and-iranian-cyber-army-in-the-name-of-ashrar-an-article-by-ashrar-team/
[45] https://www.ncr-iran.org/en/news/inside-source-reports/
[46] https://cybershafarat.com/2019/03/10/cyber-war-and-iranian-cyber-army-in-the-name-of-ashrar-an-article-by-ashrar-team/
[47] https://russiancouncil.ru/cyberiran
[48] https://phoenixts.com/blog/iranian-cyber-army-the-offensive-arm-of-irans-cyber-force/
[49] https://cybershafarat.com/2019/03/10/cyber-war-and-iranian-cyber-army-in-the-name-of-ashrar-an-article-by-ashrar-team/
[50] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[51] https://www.ncr-iran.org/en/news/inside-source-reports/
[52] https://russiancouncil.ru/cyberiran

worked on a project, called the project 910 allegedly aiming at creating a new Stuxnet virus.[53] The document outlines the development of a malware and a C2 (command and control) server. According to the report, the project intended to damage SCADA systems. The botnet was planned to act as a spy malware with identification, espionage and remote connection abilities. However, according to Clear Sky, the project was reported unsuccessful in 2016.

Under the IRGC, the Basij group operates the Basij Cyber Council.[54] The Basij group is considered a paramilitary force that comprises nonprofessional's, using volunteer hackers under IRGC specialist supervision. These volunteers are sometimes referred to as "cyberwar commandos". This body is far less organized and professional and operates only for very simple attacks. This group is included in the ground forces of the IRGC. They are constituted generally from the lowest classes of the Iranian society. Thousands of Basij fighters across the Iranian territory were provided free classes of informatics and blog creation.[55] This training serves them to answer positive comments on the Iranian regime in various communication platforms and to let believe that the government benefits from wide support. They also actively monitor the activities of potential political dissidents on social media. The Basij is specialized in the training of simple cyber activities and the recruitment of new hackers. The last cyber battalion camp was held in Abali, near Tehran.[56] In 2019, the head of the Basij announced the creation on 1,000 cyber battalion working for the regime.[57] One battalion is composed of 500 soldiers. In 2013, the Middle East Media Research Institute reported that 1,500 operatives were trained by the Basij Cyber Council. IRGC commander Hossein Hamedani stated that they "have assumed their duties and will in the future carry out many operations."[58] According to Iranian media, 15,000 members would have been trained up to now and led more than 2,000 cyber operations. 59 8,000 IT specialists would have been recruited among the Basij.

In 2019, the head of the Basij announced the creation on 1,000 cyber battalion working for the regime. One battalion is composed of 500 soldiers.

The Iranian government already uses in its kinetic operations regional proxies to decrease the responsibility of the Iranian government for the offensive actions undertaken in the Middle East. The very same rationale exists in the framework of the Iranian cyber warfare.[60] The Iranian regime uses many decentralized actors to divide the various part of an attack and dilute its responsibility, increasing the doubt from the attacked part on the appropriate

[53] https://www.clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf
[54] https://fas.org/sgp/crs/mideast/IF11406.pdf
[55] https://fas.org/sgp/crs/mideast/IF11406.pdf
[56] https://cybershafarat.com/2019/09/25/cyber-battalion/
[57] https://english.alarabiya.net/media/2019/09/08/Iran-has-thousands-of-pro-regime-social-media-accounts-
[58] https://securityaffairs.co/wordpress/35419/hacking/iran-cyber-capabilities.html
[59] https://russiancouncil.ru/cyberiran
[60] https://www.immersivelabs.com/resources/blog/iranian-cyber-capability-explained/

retaliation to launch.[61] These actors are called APT (Advanced Permanent Threat). The real origin of the attack and the State responsibility become therefore particularly difficult to assess. Their origin can be traced back to the 2000s. According to Western researchers, they were primarily used against internal targets since the Green Revolution in 2009.

According to Andersen and Sadjapour, these proxies are independent contractors with very fluctuating links with the Iranian government.[62] A group of hackers can be created or disbanded when the operation is launched or terminated. These units caninclude groups of hackers or lonely operators. This ecosystem is composed of a wide range of professionals from inexperienced hackers to private contractors working for IT companies in Iran or patriotic hackers.[63] It is sometimes even possible to find some Iranian hackers LinkedIn accounts with their recent hacking operations. They can include professional hackers or black hats (with a criminal record). It is particularly difficult to identify precisely actors in APT. Their composition can vary very quickly and overlaps between different groups. Each APT is usually created on ad hoc basis and is constituted only to carry out one single external operation (although some APT exist on a longer run).[64] Their operations are mainly concentrated on defacement, malware attacks and espionage.

According to Anderson and Sadjadpour, the Iranian APT is used by the government and IRCG to launch cyber offensives.[65] According to Levi Gundert, Sanil Chohan, and Greg Lesnewich, around 50 contractors exist and work under the orders of the Iranian state entities (with various names such as Muddy water, APT 33, APT 34, APT 39, Cobalt Gypsy, NeswBeef, Magic Hound). [66]

These APT would compete with each other or collaborate to obtain their contracts from the government. APT are paid only when the cyber mission is successful.[67] According to Recorded Future, an American cybersecurity company, the cyber offensives are segmented between various tasks which are distributed to different contractors.[68] According to this source, 2 contractors are generally used for each cyber offensives. This compartmentalization allows the Iranian government to ensure the deniability of its actions. This organization and hierarchy allows also the government to ensure the control on all the steps in the design and implementation of the cyber-attacks. This rationale is visible in all Iranian military institutions, which are also divided to avoid the emergence of for a powerful military force capable of challenging the stability of the Iranian regime.

[61] https://www.recordedfuture.com/iran-hacker-hierarchy/
[62] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[63] https://www.recordedfuture.com/iran-hacker-hierarchy/
[64] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[65] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[66] https://www.recordedfuture.com/iran-hacker-hierarchy/
[67] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[68] https://www.recordedfuture.com/iran-hacker-hierarchy/

For the regime, ideological alignment is more important than the technical skills of the proxies.[69] The biggest threat is to develop specific digital skills that could be used against the government. Therefore, the Iranian regime prefers to dilute its links with the various contractors to avoid any internal consequences and to increase the deniability of the cyber-attacks abroad. Here is the list of some of the most famous Iranian APT. Most of the Iranian APT are probably not known yet by the Western experts and only a few groups are reported by Western and Israeli cybersecurity firms.

The Ashiyane Digital Security Team was qualified by the Insikt group as a "grey hat" network security company.[70] This cyber security company was created in 2002. The official aim was to train Iranian user's to protect them from cyber vulnerabilities. The CEO of this security company is Behrooz Kamalian, considered "the father of the Iranian hacking" and claimed openly his intention to train new Iranian hackers. A forum linked to this company gathers an online community specialized in cybersecurity and Iranian hackers. 20,000 users were reportedly benefitting from the services of this forum. The company proposes training in ethical hacking systems as well as software tests to seek for vulnerabilities in Iranian companies. It offered a training hacking course on Linux and Windows in a course named security and counter infiltration. This company launched in 2009 a massive cyber-attack against 700 Israeli websites to retaliate against the invasion in Gaza. It launched also numerous hacking actions, notably against the Thai, Indian government organizations, against Saudi Arabia, Israel and the U.S.

The Iranian Cyber Army (ICA) is one of the oldest and most persistent Iranian APT. According to Western researchers, this APT was directly linked to the IRGC but no official declarations confirmed this link.

Behrouz Kamalian has claimed that while Ashiyane Forum operates independently and spontaneously, they cooperate with the Iranian military apparatus in advising and improving security, and "have always operated in the framework of the goals of the state."[71] The U.S. Department of Justice accused the Ashiyane Digital Security Team of launching cyber-attacks on the behalf of the IRGC. Some experts suspect cooperation between the Ashiyane and FATA to trace political opponents on social media and the Internet.[72] Moreover, according to the Iranian criminal code at articles 725 and 75, the selling of hacking tools is punished. The Ashiyane group has never been prosecuted despite the selling of these products on its forum.

The Iranian Cyber Army (ICA) is one of the oldest and most persistent Iranian APT. According to Western researchers, this APT was directly linked to the IRGC but no official declarations

[69] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[70] https://www.recordedfuture.com/ashiyane-forum-history/
[71] https://www.securityweek.com/rise-and-fall-ashiyane-irans-foremost-hacker-forum
[72] https://russiancouncil.ru/cyberiran

confirmed this link.[73] Fars News Agency reported its existence in 2009.[74] This information was confirmed by FireEye, an American IT security company. The Iranian press suggested that the group could be linked to the IRGC in 2010. It is very difficult to assess precisely the composition of this group. According to Western researchers, the group would be composed of young IT experts in hacking surveillance and professional hackers that trains amateurish hackers.

Experts estimate that this body includes 3,000 fighters.[75] According to international experts, the Iranian government officials refer to using it to hack "enemy sites," diverting Internet traffic and hacking into foreign media sites and social media platforms.

The former IRGC commander in Tehran stated in 2012 that the Cyber Army opened two cyber war centres in Tehran under the aegis of the IRGC.[76] It is not clear whether he referred to the ICA in this declaration. According to Al Arabiya, an Emirati media, the head of the ICA is believed to have been Mohammad Hussein Tajik, a Quds force member until his death.[77] He was killed allegedly by governmental forces. According to this source, he was tortured and imprisoned for having collaborated and shared information with members of the Green movement. Al Arabiya reported some information from a political opponent, Roohollah Zam, currently living in Paris. According to this source, the ICA formed the foundation of the Khaybar Centre for Information and Technology in 2011. Its official website is Ghassam.ir.

Massive cyber offences were attributed to the ICA such as a defacement campaign against Twitter in 2009 and Baidu in 2010 as well as against the Voice of America in 2011.

The group is allegedly cooperating with other Iranian entities linked to cyber warfare. This group is suspected to be behind the cyber-attack against the Digi Notar, a Dutch web security firm in September 2011. The Iranian hackers have managed to obtain the certifications accesses illegally giving them access to information on 300,000 Iranian Gmail accounts. This attack was carried out to monitor the activities of Iranians on the Internet and their private emails.

Other massive cyber offences were attributed to the ICA such as a defacement campaign against Twitter in 2009 and Baidu in 2010 as well as against the Voice of America in 2011. The ICA was also reportedly at the origin of the wide cyber-attack targeting Turkey's electric grids, which were put out of service for 12 hours among its 44 provinces.[78, 79] American experts accused also the ICA to be responsible for the cyber-attack against the New York

[73] https://russiancouncil.ru/cyberiran
[74] https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf
[75] http://www.persianpasdaran.com/#/
[76] https://www.recordedfuture.com/iran-hacker-hierarchy/
[77] https://english.alarabiya.net/features/2017/01/15/Secrets-and-activities-of-Iran-s-electronic-army
[78] https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf
[79] https://russiancouncil.ru/cyberiran

dam in 2013.[80] International experts also suspect that this entity cooperated with foreign entities to damage American assets. According to American sources, before 2010, the ICA paid Chinese and Russian professional hackers to launch attacks on its behalf.[81] Some experts also suspect collaboration between the ICA and Hezbollah.

The ICA is also very active against internal targets. The ICA hacked the accounts of Mohsen Sazegara, and Iranian journalist and Iranian media such as Farsi 1.

The Sun Army is also an old APT in the Iranian cyber ecosystem. The group is reportedly linked to the IRGC cyber activities, and was detected first in 2010. According to the NCRI, the group was made of a core 6 hackers according to NCRI.[82] 3 members were prosecuted by the US department of Justice for their responsibility in the Ababil attack in 2012. They reportedly blocked 500 sites and Iranian accounts on Twitter and Facebook in a separate attack.

Magic Kitten is allegedly the oldest and most elaborate APT from Iran. Western experts estimate that this APT is related to the MOIS, rather than IRGC.[83] The group was created in 2007 and is still active. Magic Kitten is said to have designed and launched malware attacks against dissidents such as against the journalist Vahir Ostad and Turkish asylum forums for Syrian refugees. Some experts think that Magic Kitten sent some malware to the Cyber Hezbollah.

The Ajax security Team was identified by the security company FireEye in 2010 and achieved to detect some hackers (such as Car3X, HuRR!C4nE, Oday, Mohammad PK and Crim3r).[84] The APT has set up a forum gathering the experience of 256 registered hackers in Iran (in 2018). It is one of the rare APT that could design its own software for its attacks. Ajax is one of the most active and professional hacker group among the Iranian entities although the level of its cyber attacks was deemed unsophisticated by Western experts.

Rocket Kitten was reportedly created in 2011 and identified in 2014 by CrowdStrike, an American cybersecurity company.[85] According to the cyber security company CheckPoint, Yasser Balani is the coordinator of this APT.[86] This group is thought to be specialized in operations against Middle Eastern security firms as well as intelligence gathering and information and cyberespionage. According to ClearSky, it was responsible for the cyber-attacks against 5500 targets in the Middle East. It was held responsible for the operations

[80] https://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543
[81] https://cybershafarat.com/2019/03/10/cyber-war-and-iranian-cyber-army-in-the-name-of-ashrar-an-article-by-ashrar-team/
[82] https://www.ncr-iran.org/en/
[83] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[84] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
[85] https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions
[86] https://www.scmagazine.com/home/security-news/supposed-mastermind-behind-rocket-kitten-apt-identified-in-research-paper/

Saffron Rose, Newscaster and Woolen Goldfish. The group allegedly helped the IRGC to collect information on the Obama administration and launch spear-phishing attacks against Facebook profiles of American government employees. Clear Sky reported in 2017 an operation from this group called Wilted Tulip which used spear-phishing and commercial malware. The group was disbanded in 2014. Some experts think that it mutated into another Iranian APT, Charming Kitten. For some experts, Rocket Kitten would be linked to the Ajax team.[87] Members of the Ajax Team would be also present in the group Rocket Kitten according to CheckPoint, an Israeli cybersecurity company.

Flying Kitten was a group created around 2009 and created primarily as a patriotic hacking group. The company Crowd Strike estimates that Flying Kitten was a mutation of the Ajax security team and Rocket Kitten. The company FireEye suspects the involvement of this APT in the Saffron Rose attack, a cyber operation against American defence and aerospace companies.[88]

Charming Kitten was created in 2014 and is allegedly specialized in cyber espionage and social media, and the design of fake websites for spear-phishing operations.

This APT would have refocused its activities on cyber-espionage between 2013 and 2014. The group was able to design and use its own malware. The group also hires individuals and contractors to launch censorship actions and espionage. According to Anderson and Sadjapour, this group was in reality connected to Rocket Kitten.[89] Clear Sky correlated this group with the activities of Charming Kitten.

Charming Kitten was created in 2014 and is allegedly specialized in cyber espionage and social media, and the design of fake websites for spear-phishing operations. According to Mandiant, an American cybersecurity company, this group was be well-financed by the government.[90]

Copy Kitten, is reportedly one of most performant APT. According to Western sources, it used the same tools and modus operandi as Rocket Kitten. This APT mainly performs espionage attacks against foreign institutions since 2013. It used watering holes[91] to attacks Israeli targets, media, infect the links to attack people linked to these media, against private agencies in the whole Middle East, Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany.

[87] https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf
[88] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
[89] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
[90] https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions
[91] A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.
Source: https://searchsecurity.techtarget.com/definition/watering-hole-attack

Occasionally individuals in other countries are targeted as well as UN employees. Clear Sky reported in 2017 an attack from this group against the German Bundestag.[92] The Israeli company suspects that Copy Kitten launched the Wilted Tulip operation and was the same group as Rocket Kitten.

Helix Kitten (or Oilrig) is one of the most active APT and operates against Middle Eastern, African and U.S. targets. The group was identified by Palo Alto Networks, an American cybersecurity company. It acted under the aegis of the MOIS and IRGC. The group did not launch internal cyber espionage and censorship. This APT specialized in spear-phishing messages to deliver malware, steal information. Its technics are reportedly not very sophisticated. The APT have been able to use some tools leaked from the American NSA and uses other malware created on its own.

Magic Hound is an APT also identified by the Palo Alto Networks. This APT have targeted mainly governmental agencies in Saudi Arabia. It was linked to the APT Rocket Kitten.

The APT Cutting Sword of Justice is the Iranian actor that claimed responsibility for the Shamoun attack on Saudi Aramco and RasGas in Qatar in 2012. Cyber experts could not gather much information on this APT. The group was reportedly dissolved after the 2012 attack. Its activities resumed with the other Shamoun attacks in 2016 and 2018, with the use of rebranded malware. The same rationale does exist for the group Iz ad Din al Qassam, the Iranian APT at the origin of the Ababil cyberattack against the American financial sector between 2012 and 2014. The U.S. Department of Justice could identify some members at the origin of this attack.

Elfin or APT 33 is a group active since 2015 which is specialised in energy and defence fields and launched attacks against SCADA systems to control the infrastructures.

In 2015, Lab Dokhtegan, a Telegram channel, disclosed the existence of a new Iranian APT, called Oilrig or APT 34. The channel would have also disclosed previously the existence of Rana, another APT also reported by Clear Sky.[93] APT 34 have launched attacks mainly against Middle Eastern supply chains. Later, another Telegram channel, Green Leaks, along Lab Dokhtegan disclosed the tools used by another APT called Muddy Water.

Elfin or APT 33 is a group active since 2015 which is specialised in energy and defence fields and launched attacks against SCADA systems to control the infrastructures. According to FireEye, this group is financed and supported by the government.[94] It targets mainly vulnerable infrastructures in Saudi Arabia, South Korea and the U.S. Clear Sky suspects that the APT Shamoun is in reality APT 33.

[92] https://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf
[93] clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf
[94] clearskysec.com/wp-content/uploads/2019/05/Iranian-Nation-State-APT-Leak-Analysis-and-Overview.pdf

In 2019, the Microsoft Threat Protection Intelligence Team identified the group Phosphorous.[95]It is said to have targeted the previous candidates of the U.S. presidential campaign in 2016. They launched spear-phishing campaigns aiming at gathering information on American candidates.

According to Western researchers, private companies are particularly involved in this ecosystem. They are particularly useful for the Iranian regime to circumvent the U.S. restrictions to steal data. According to Collins and Sadjapour, it is visible that Iranian firms are also operating for cyber-attacks due to the rhythm of their actions (some cyber campaigns were very active during the workweek and dormant during the Iranian Holidays).[96]

Universities and educational institutions also participate in Iranian cyber operations and in the training of these hackers.

The American government accused several companies and private firms of cyber-attacks and imposed sanctions against them. It is the case for the Ajily software procurement group which was classified by the U.S. Department of Treasury as an international organized criminal group.[97] According to the Wisconsin Project, this company run by Mohammad Saeed Ajily managed to steal some software from an American engineering company.[98] This software has potential application in the guidance systems for the Iranian missiles.

The Mersad Company and IT security Team which is allegedly involved in the DDOS attacks against the American banking system in 2013 were also targeted by American sanctions. 7 employees from this company were indicted by the U.S. Department of Treasury.[99] The latter company is reportedly affiliated to the IRGC.

Universities and educational institutions also participate in Iranian cyber operations and in the training of these hackers. Most of Iranian universities are now proposing lectures and courses in IT technologies.[100] The Sharif industrial university is, for example, designing lectures in hacking techniques and delivers courses on cyber security and counter infiltration program.[101] A cyber war course is allegedly proposed since 2013 by military universities in Iran.[102] The Khomeini University, directly linked to the IRGC proposes also a degree in cyber security and organizes conferences on this topic. Some universities are provided research centres, such as the research institute in cyber space in the Shahid Basheti University and the advanced information and communication technology centre in the Sharif University.[103] The Imam Hossein University, the Isfahan and Amir Kabir, Shiraz, Mabna and Amir Kabir

[95] https://en.radiofarda.com/a/microsoft-details-sophisticated-hacking-linked-to-iranian-cyber-espionage-group/30689747.html
[96] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[97] https://www.treasury.gov/press-center/press-releases/Pages/sm0125.aspx
[98] https://www.iranwatch.org/iranian-entities/ajily-software-procurement-group
[99] https://www.treasury.gov/press-center/press-releases/Pages/sm0158.aspx
[100] https://www.article19.org/ttn-iran-november-shutdown/
[101] https://cybershafarat.com/persian-pasdaran/
[102] https://russiancouncil.ru/cyberiran
[103] http://en.sbu.ac.ir/Research_Institutes/CyberspaceResearch/Pages/default.aspx

universities are also participating in the training of Iranian students in these fields. 20% of all Iranian students are enrolled in such courses. In 2011, more than 2 million Iranian students were specialized in IT.

According to Western researchers, these universities aim at training the new hackers for the Iranian groups and APT.[104] Internships would be proposed to students within Iranian hacker groups or within the Basij Cyber Council. The Ayatollah Khamenei already referred to students in IT as the Iranian cyber agents: "You are the cyber-war agents and such a war requires Ammar-like insight and Malik Ashtar-like resistance."[105]

Some of them directly train new hackers such as the Shahid Beheshti University and the Imam Research institute cyber space Shahid Besheti University

Some universities were directly involved in external cyber-attacks. According to the U.S. Department of Treasury, the Mabna Institute is a private government entity contractor created by Gholamreza Rafatnejad and Ehsan Mohammadi in 2013 and is located in Tehran. The institute was designed to help Iranian universities to get scientific documents from foreign centres and universities. It targeted foreign universities to steal non-Iranian scientific research documents by computer intrusions.

Through the theft of personal identifies of researchers and members of foreign educational institutions, they could steal relevant researches that are sold later on Iranian online platforms. In total, 100,000 accounts were targeted from professors around the world. The Mabna Institute is linked to Iranian universities. According to the U.S .department of Justice, The Mabna Institute, attacked universities from the U.S., Australia, Canada, China, Denmark, Finland, Germany, Ireland, Israel, Italy, Japan, Malaysia, Netherlands, Norway, Poland, Singapore, South Korea, Spain, Sweden, Switzerland, Turkey and the United Kingdom. This operation was carried out between 2013 and 2017. The main targets were expensive online libraries whose accesses were prohibited for Iranian institutions due to American sanctions. The Mabna institute achieved to access to repository information and main online libraries representing 31 TB of data. International experts estimate that these data were used in the interests of the Iranian IRGC. They were sold on two other online platforms such as megapaper.ir and gigapaper.ir. In 2018, 9 members from this institute were indicted by the U.S. Department.

Finally, some independent hackers can be found. For international experts, they represent the category of patriotic hackers.[106] However, their relations with the government remains blurred and it is not possible to check if their actions are directly led by other contractors, themselves or working for the government.

[104] http://en.sbu.ac.ir/Research_Institutes/CyberspaceResearch/Pages/default.aspx
[105] https://www.haaretz.com/iran-s-ayatollah-prepare-for-cyber-war-1.5321907
[106] https://www.haaretz.com/iran-s-ayatollah-prepare-for-cyber-war-1.5321907

Iranian hackers also cooperate with foreign hackers' groups across the Middle East to target the assets of their common enemies. The links between these groups are not officially claimed in Iran. International cyber experts could retrace some footprints proving the collaboration of the Iranian regime with hackers among its regional proxies. It should be noted that overall, the cyber cooperation with Iranian external proxies is not as developed as Iranian kinetic operations with Hezbollah, Houthis, or the Iraqi PMF.

Iranian hackers also cooperate with foreign hackers' groups across the Middle East to target the assets of their common enemies.

The Hezbollah Cyber Army could be linked to the capabilities of Iranian hackers.[107] According to some experts, its real capabilities are not known. However, some experts stated that the capabilities of this group are superior to the Iranian one in terms of sophistication. Hezbollah's hackers were primarily concentrated on the propaganda and expanded their activities to psychological warfare, recruitment, messaging, and misinformation. A special unit is specialized in Psychological warfare. According to Michael Eisenstadt, the director of The Washington Institute's Military and Security Studies Program, Hezbollah's hackers became performant in misinformation due to the wars against Israel in 2000 and 2006, when Hezbollah's operatives launched a psychological operation to undermine Israel defense forces' (IDF) morale.[108, 109] In 2006, during the 34-day war against Israel, Hezbollah's operatives used sophisticated cyber-attacks against websites from multiple countries which supported the Israeli's actions in Lebanon.[110] IDF tried to cut the Internet in Lebanon to impede the actions of Hezbollah. In 2006, the Hezbollah Cyber Army was reportedly created and gathered professional hackers.

In 2013, experts reported the formation of the Islamic Cyber resistance (ICR) in the wake of the killing of a Hezbollah commander Hassan Laqiss by the IDF.[111] The group launched a cyber offensive against Israeli intelligence. On January 7, 2014, the ICR stated that they stole information from the Local Area Network (LAN) of the Israel Airports Authority (IAA).[112] This sensitive information concerned domestic and international flight maps. International cyber experts estimate that Hezbollah's operatives are leading this group. The composition of its members is not known. This group has alleged links with the Syrian Electronic Army. On August 10, 2013, the ICR and the Syrian Electronic Army (SEA), a pro-Assad hacker group, attacked a Kuwait mobile operator (Zain Group) and leaked information that included passwords.[113] The ICR has no Facebook or Twitter accounts. However, it seems that WikiLeaks.ir and @quickleak.org on Twitter are the main platforms for their leaks.

[107] http://strategicstudyindia.blogspot.com/2018/02/hezbollah-goes-on-cyber-offensive-with.html
[108] https://www.thecipherbrief.com/cyber-irans-weapon-of-choice-2
[109] https://vudailleurs.com/le-cyberespace-le-conflit-entre-israel-et-le-hezbollah/
[110] https://vudailleurs.com/le-cyberespace-le-conflit-entre-israel-et-le-hezbollah/
[111] https://www.trackingterrorism.org/group/islamic-cyber-resistance-icr
[112] https://www.cognyte.com/blog/?cat=31
[113] https://www.recordedfuture.com/islamic-cyber-resistance-activity/

Iran actively supports the actions of the Hezbollah Cyber group. Since 2010, Tehran hosts the Cyber Hezbollah conference and invites Hezbollah's commanders. For cyber experts, it is clear that Iran trains and assists Hezbollah's officers in their cyber activities. Anderson and Sadjapour reported that Hezbollah's operatives allegedly used a malware created by the Iranian APT Magic Kitten.[114] The Iranian IT Sec Team would have also helped the Hezbollah's operatives. According to the Israeli firm Check Point, Hezbollah's operatives would have achieved to create their hacking toolset. The Iranian media Fars News agency regularly reports the Hezbollah's cyber offensives and communicates on this topic along the al Manar news agency led by Hezbollah's operatives.

Iran actively supports the actions of the Hezbollah Cyber group. Since 2010, Tehran hosts the Cyber Hezbollah conference and invites Hezbollah's commanders.

Cyber Hezbollah could launch by itself some cyber operations. The operation Volatile Cedar was launched in 2015 and targeted private and public entities in the Israeli defence sector with a malware.[115] Some experts suspected the presence of some employees from the Iranian IT security company. The operation targeted also Lebanese state institutions. Hezbollah's hackers are still launching sporadic attacks against Saudi and Israeli critical infrastructures. It is more specialized in espionage rather than sabotage operations. In 2017, intelligence services from Czech Republic neutralized servers used by Hezbollah to diffuse malware against Middle Eastern and European targets.[116]

The Syrian Electronic Army was reportedly created just after the first Syrian demonstrations in 2011.[117] It claimed on social media that it is not linked to the Syrian government and withdrew these declarations afterwards. The group is specialized in web defacement, malware attacks, DDOS, phishing and espionage operations. It targets mainly internal opposition groups in Syria and Western news agencies. In 2013, the SEA hacked the AP Twitter account of the White House, claiming that there was an attack and Obama wounded.[118]The declaration caused the drop in the stock market by 136 billion dollars. The group also targeted the NYT Twitter account and Huffington post-UK in August of the same year. The group disappeared in 2014 and rebooted its actions from 2016. It increased its cyber operations against Western media outlets, Human rights organization, communication platforms and American military websites. In 2017 the SEA shifted its strategic structure and became the public relations arm of the government.[119] The group launches more disinformation operations and DDOS attacks.

[114] https://www.recordedfuture.com/islamic-cyber-resistance-activity/
[115] https://www.cyberdefensemagazine.com/volatile-cedar-the-cyber-espionage-campaign-from-lebanon/
[116] https://www.zdnet.com/article/czech-intelligence-service-shuts-down-hezbollah-hacking-operation/
[117] https://opencanada.org/new-face-syrian-electronic-army/
[118] https://www.nbcnews.com/news/other/syrian-electronic-army-seen-nuisance-not-serious-cyberthreat-f8C11042663
[119] https://foreignpolicy.com/2013/09/04/how-did-syrias-hacker-army-suddenly-get-so-good/

The SEA is reportedly a loose team of hackers linked to the Assad's forces. Its self-proclaimed commander is allegedly Yaser al Sadeq.[120] The group is considered as a non-institutionalised militia but has an emblem and already organized some parades along with other Assad forces. It pleaded allegiance to the regime of Bashar al Assad.[121] Several branches exist within the SEA such as the Golden Rat group, known as APT-C-27 which leads attacks against the Syrian opposition forces and the Pat Bear, or APT-C-37 which organized attack against the ISIS and Syrian opposition forces, more particularly in Idlib region. Moreover, the government implemented other instruments that are correlated to the SEA such as the Syrian Cybercrime court which prosecute Syrian individuals according to the 2012 Internet law and the Syrian division for combatting cybercrime which arrested already 140 people.

According to Michael Hayden, the former Director of CIA and NSA the SEA would have strong links with the Iranian cyber ecosystem. The SEA would be linked to Group 5, which is present among other Syrian hackers.[122] Cyber experts noticed that this recent operator used Persian language and Iranian hosting companies. The group realized watering holes attacks against Syrian opposition forces. The group would use also Iranian malware and would be active on the Iranian hacking forums such as Ashiyane group.

The Yemen Electronic Army is another hacker group which could have some links with Iranian hackers. It emerged in 2015 and engaged in two cyber operations directly against Saudi Arabia.[123] The first one was the attack against the al Hayat media in April 2015.[124] The second one was the operation against the Saudi Minister of Foreign Affairs in 2015 and leaked the stolen documents on Iranian media. The group hacked the Al Alam Twitter account in 2015. These attacks were reported quickly by Iranian media such as Pastebin which published the leaked documents. The group tends also to use Iranian websites to communicate on their attacks such as in Parastoo and Quickleak.ir. According to cybersecurity experts, the group could have been trained directly by Iranian hackers. Other cybersecurity experts even suspect the presence of the Iranian cyber army behind the existence of the group. The Yemeni group uses also the very same phrase as Iran during the operation Shamoun targeting Saudi Arabia (the Cutting Sword of Justice). Moreover, the attack against the Saudi Minster was suspicious regarding the sophistication of the attack. An external help would have been probably required. It is impossible with OSINT researches to retrace the presence of members of the Yemeni hackers' group before 2015.

[120] https://opencanada.org/new-face-syrian-electronic-army/
[121] https://vyagers.com/2019/12/04/uncover-the-secrets-of-the-syrian-electronic-army-the-role-and-influence-of-cyber-attacks-in-the-syrian-civil-war/
[122] https://citizenlab.ca/2016/08/group5-syria/
[123] https://www.vice.com/en/article/wnj9gq/theres-evidence-the-yemen-cyber-army-is-actually-iranian
[124] https://english.alarabiya.net/media/digital/2015/04/14/Pan-Arab-newspaper-al-Hayat-hacked-by-Yemen-Cyber-Army-

3. Iranian cyber tools and modus operandi

The nature of attacks can be divided between espionage and sabotage. Contrary to Chinese and Russian attacks, Iranian cyber external operations are mainly designed to cause only destructive damages against critical infrastructures. Intelligence operations are mainly led at the internal level. The Iranian armed forces are developing various tools for these two categories of offensive operations.

It is however difficult to assess precisely what are the real Iranian cyber capabilities and tools available. To increase its deterrence power and to palliate the lack of technical capabilities, the Iranian regime boasts its capabilities regarding its cyber skills, blurring the real technical means available to Iran. The same rationale can be found concerning its missile program and serves to increase the deterrence power despite a potential lack of sophisticated tools.

However, cyber experts estimate that the tools used by the Iranian cyber ecosystem cannot be compared with the tools employed by Chinese and Russian hackers. The Iranian techniques in cyber espionage and sabotage are very rudimentary. Most of the hackers rely on tradecraft and persistence to succeed in their cyber-attacks.[125] According to Western cyber experts, the cost for a cyber weapon in Iran is estimated between 300 and 50,000 dollars. However, this technological gap does not hamper Iranian hackers to obtain efficient results against foreign enemies. Moreover, it seems that these rudimentary tools are particularly efficient against the Iranian population. At the external level, the Iranian cyber weapons can attack any targets in the globe with a high level of deniability and still put at threat critical infrastructures in Western and Middle Eastern countries.

The Iranian techniques in cyber espionage and sabotage are very rudimentary. Most of the hackers rely on tradecraft and persistence to succeed in their cyber-attacks.

For its internal information and espionage operations, Iranian hackers rely mainly on filtering systems to monitor the activities of the Iranian population on social media and on the Internet.

The first kind of attack that Iranian hackers are employing is the distributed denial-of-service (DDOS) which aims at rendering a website inaccessible and overload by huge traffic.[126] The cybersecurity company CloudFlare defines this attack as "a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic." This type of attack can cause the disruption and financial losses for the targeted victims. The operation Ababil carried out in 2012 against the American financial system is a case example of this kind of offensive.

[125] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[126] https://russiancouncil.ru/cyberiran

American banks had to finance new security systems to protect themselves from such strikes, an investment which cost 10 million dollars.

Another type of basic cyber-attacks is defacement campaigns. Iranian hackers often employ this technique to take control of a website and modify its content. The aim is usually to put information that is aligned with the views of the Iranian government or to degrade the image of its adversaries.

Iranian hackers also regularly launch spear-phishing and phishing attacks with fake personas and social engineering tools or specifically designed emails. These attacks serve to obtain the control on email accounts and access to various data. It is particularly used against internal targets. The hackers lure the victims with fake links to get their password and obtain their personal information. Charming Kitten would have launched 2,000 spear-phishing attacks with accounts on social media with fake personas network.[127] These attacks could be made with ICloud services as well. Iran launched a cyber-attack against U.S. employees from the American presidential campaign in 2016.[128] It achieved to penetrate personal accounts and steal personal information thanks to this method. Earlier, Iran launched spear-phishing attacks against members from the Obama administration which were part of the Iranian Nuclear deal negotiation deal.[129] The Iranian government also uses website defacement at an internal level to discredit opposition media. The Iranian hackers create fake opposition media with wrong information to decrease the popular support to these media. It spreads also rumors on opposition media on Telegram and other social networks.

Iranian hackers also regularly launch spear-phishing and phishing attacks with fake personas and social engineering tools or specifically designed emails.

Iranian hackers developed rudimentary malware that is not as sophisticated as Western malware launched against Iran. The Stuxnet attack was a milestone in the design of cyber operations by Iran. According to the American National Security Agency (NSA) Iran achieved to reverse-engineer the Stuxnet virus and would be able to launch a cyber-attack using this tool.[130] The Stuxnet virus spread to other countries in Europe as well. The virus helped Iran to build its own malware and software. The Shamoun malware is one of the most famous tools used by the Iranian hackers served to attack the SCADA system of the oil facilities forms the Aramco in Saudi Arabia in 2015. Other malware reportedly shared some similarities with other ones such as Flame and Duqu. According to Kaspersky Lab, the same Iranian APT could have been the authors of the same tools. Flame is a malware designed for espionage operations and discovered in May 2012 by the Iranian Oil Ministry. According to a report from

[127] https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions
[128] https://www.reuters.com/article/us-cybersecurity-iran-exclusive/trump-re-election-campaign-targeted-by-iran-linked-hackers-sources-idINKBN1WJ1ZM
[129] https://russiancouncil.ru/cyberiran
[130] https://www.zdnet.com/article/hard-disk-wiping-malware-phishing-and-espionage-how-irans-cyber-capabilities-stack-up/

the Centre of Security Studies, Flame would be able to scan documents," turn on the microphone and register conversations, scan for Bluetooth-enabled devices in the vicinity, and take screenshots".[131] Duqu is a Trojan malware that shares some similarities with Stuxnet and Flame.[132] It targets Industrial Control Systems (ICS). Its existence was reported since 2011. More recently, IBM researchers discovered in 2019 a new malware, named Zero Clear," that would have been created by the Iranian APT 34.[133] It would target companies across the Middle East. The malware would have been used in cyber-attacks against the Bapco Company in Bahrain.

The Iranian hackers also use pirate versions of professional penetration to conduct cyber campaigns. Iran reportedly acquired hardware from foreign malware from Chinese telecom firms and Russian cybersecurity firms. For example, the Chinese company ZTE was suspected in 2010 to have sold monitoring software to Iranian telecommunications companies. [134]

Iranian hackers may also find publicly available tools and commercial tools to build their malware. However, these tools open some vulnerability for Iranian hackers. The versions are very often outdated and the malware are already known in the West and is already protected against them.

Since 2012, the Iranian government fosters the development of national software and malware. For example, the use of anti-virus software was prohibited from 2012.[135] 200 Iranian IT companies endeavored to develop this national software and National-linux based systems.

Moreover, according to the Project Pistachio Harvest from the security company Critical Threats, Iranian hackers would also be able to acquire software and hardware from the U.S. and Europe by proxying" online infrastructures through American companies" or Internet service providers.[136] The Project described the actions of the Ashiyane group that achieve to proxy its IP addresses through the American company CloudFlare Inc or XL Host. 11 IP addresses and hundreds of domains from Iranian APT were registered in the U.S., allowing them to acquire hardware, software and cloud systems that Western countries wanted to deny Iran.

Iranian hackers must always renew their approaches to use these techniques against foreign targets on the long run. Indeed, foreign targets with higher financial means allocated for their cybersecurity can quickly adapt to the Iranian rudimentary attacks. The lack of sophistication of these tools drives Iran to adopt an opportunistic cyber strategy based more on frenetic

[131] https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions
[132] https://phys.org/news/2011-11-iran-duqu-malware.html
[133] https://www.zdnet.com/article/iranian-hackers-deploy-new-zerocleare-data-wiping-malware/
[134] https://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322
[135] https://russiancouncil.ru/cyberiran
[136] https://www.criticalthreats.org/analysis/the-growing-cyberthreat-from-iran-the-initial-report-of-project-pistachio-harvest-5a4408f5949b0

attempts rather than on a real pre-established target plan. Iranian hackers are therefore more cashing in from the vulnerabilities of its adversaries rather than on its strengths. Having said this, it should be however emphasized that the Iranian attacks were sometimes very costly although they are not very sophisticated. The operation Ababil cost 10 million dollars to the American banks that needed to invest in more protective systems. The operation against the Aramco facilities impeded the trade exchange between the Saudi oil firm and external partners for 5 months. None states benefit from a perfect cyber protection and Iranian hackers rely on these gaps to keep on their attacks.

Cyber tools are even more efficient against Iranian targets. The Iranian regime uses all the parts of the Iranian cyber ecosystem to control, censor and arrest the potential dissidents.

The Iranian cyber police use software like Black Spider to investigate accounts of social media and messages to arrest people who criticized the government.[137] The Iranian regime also launches distribution malware Trojan, spyware on Telegram and Café Bazaar, an app market for android developed by the government.[138] Iranian hackers also target dual nationals and businessmen who were arrested by the IRGC to target their social accounts and obtain information on their contacts. The arrest of Siamak Namazy, an Iranian Emirati-based energy consultant is an example of such a tactic. He was arrested by the IRGC in 2015. According to cyber experts, the APT Rocket Kitten would have hacked his Facebook and Google accounts to send messages to his contacts and obtain sensitive information.[139] With this operation, Rocket Kitten achieved to compromise a lot of important scholars, journalists and department employees. Babak Zanjani is an Iranian-Danish businessman billionaire who was arrested by Iranian forces under allegations of corruption in 2013.[140] His death sentence was commuted only if he accepted to cooperate with the Iranian government.[141] In the wake of his arrest, a wave of cyber-attacks targeted the employees of his company, Sorinet through the iCloud service.

The Iranian cyber police use software like Black Spider to investigate accounts of social media and messages to arrest people who criticized the government.

The Iranian regime also controls access to the Internet by Iranian people since 2009. In 2010, the government launched a governmental program to control the Internet and to foster its digital sovereignty.[142] This project could be compared to the Russian plan to create an Internet network for Russian users only and that would be blocked for external users in parallel to the international network. The Iranian project was first launched by Reza Taighipour, with the creation of a national Iranian network with its search engines, market

[137] https://www.hackread.com/how-iran-traps-its-facebook-users-with-black-spider/
[138] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[139] https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134
[140] https://www.bbc.com/news/world-middle-east-25551849
[141] https://www.reuters.com/article/us-iran-billionaire-sentence-idUSKBN13S09P
[142] https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf

apps. The Iranian regime created its entity to control the use of the Internet called the Iranian National Information Network (called SHOMA in Persian). This tool was coined under the presidency of Rouhani who was accused by hardliners of being too lenient with the Internet use and not responsive enough regarding the internal threats represented by the free use of the Internet by Iranian people. This cyberspace would be accessible only from the Iranian territory. The Iranian government also restricted the access of foreign communication app and replaced them by its Iranian apps such as Soroush and Bale and national search engines replacing google such as Ya Magh! (standing for my God!). According to the Survey, in 2012, 27% of Iranian websites are blocked in Iran. According to Ahmad Ali Montazeri, the head Internet censorship committee, Iran banned 14,000 websites and social media accounts in 2016.[143]

This project has not been fully realized but the Iranian government achieved also to impose strong censorship within its territory.

The Iranian legislation is extremely weak regarding the data privacy and protection, allowing the regime and the cyber ecosystem to impose very strict monitoring and censorship among Iranian Internet users.[144] The regime prohibited the use of VPN by the population which could have allowed them to bypass these restrictions. The regime also forces IT companies to share their data on Internet customers. During the demonstrations in 2017, 2018 and 2019, the regime blocked websites and communication platforms and an increase of cyber-attacks was reported. Because of the last demonstrations in 2019, triggered by the increase of gas prices, the Iranian government shut down the Internet for one week.

The Iranian legislation is extremely weak regarding the data privacy and protection, allowing the regime and the cyber ecosystem to impose very strict monitoring and censorship among Iranian Internet users.

4. External help

There is no official proof regarding the commitment of a foreign country to the development of the Iranian cyber warfare. There are, however, some suspicions regarding the role of China and North Korea in the Iranian cyber program.

China is the main country that could help Iran to develop its toolset. The former is Iran`s biggest trade partner and already violates American sanctions regarding the import of Iranian oil or the assistance to develop its missile program.[145] In 2019, the Iranian ministry of ICT Mohammad Javad Azari Jahomi, met his Chinese counterpart, China Miao Wei, to discuss

[143] https://english.alarabiya.net/media/digital/2016/12/08/Iran-bans-14-thousand-websites-and-accounts-weekly-

[144] https://russiancouncil.ru/cyberiran

[145] https://www.iranwatch.org/our-publications/weapon-program-background-report/history-irans-ballistic-missile-program#Foreign%20Suppliers

their common cyber vulnerabilities.[146] They also commonly accused the U.S. of leading a hegemonic position on the cyber sphere.

In 2011 ZTE, the largest telecom supplier in China and a company affiliated to the Chinese government would have helped the Iranian government to develop its monitoring systems on the Internet.[147] This company is specialized in the surveillance market. The company would have sold to the Telecommunication Company of Iran (TCI) in 2010, a monitoring package, called the 2XMT, efficient on social media.[148] The package includes also deep packet interception and intrusive technologies. These technologies are useful to monitor the Internet traffic and content. The TCI would have paid 98.6 million euros for these transfers.

Moreover, the ZTE Company was accused in 2017 by the U.S. of having sold American hardware to Iran (from Microsoft, Oracle, Dell, Cisco and Symantec companies for example). The ZTE Company already traded with American companies that did not know the existence of commercial links with the TCI. The Chinese company paid 892 million dollars to American companies to repair the damage caused.

North Korea could have helped Iranian hackers. However, no proof exists to corroborate this suspicion.[149] North Korean scientists are already helping Iran to develop its missile and nuclear programs. According to a report released by Cylance, an American cybersecurity company, Iranian hackers could have worked outside their country and served other countries.[150] In 2012, the two countries reached a scientific and technical agreement that called for the "exchange of expertise" and "joint use of scientific research equipment." This agreement was compared by some experts to the agreement reached between Syria and North Korea in 2002.[151] In the wake of this agreement, Iranian hackers attacked American financial institutions in the framework of the Ababil Operation. Moreover, Claudia Rosett, a Journalist with the Foundation for Defence of Democracies noticed similarities between the Iranian attack against the Las Vegas Sand Corporation and the Korean cyber-attack in 2014 against Sony entertainment.[152] According to a report from the U.S. department of defence released in 2017, Iran and North Korea would have significantly improved their respective cyber capabilities.[153]

[146] https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/?sh=2e9034ac42eb
[147] http://graphics.thomsonreuters.com/12/03/IranChina.pdf
[148] https://www.reuters.com/article/us-zte-iran-aryacell/exclusive-chinas-zte-planned-u-s-computer-sale-to-iran-idUSBRE8390T720120410
[149] http://www.thetower.org/article/how-iran-and-north-korea-became-cyber-terror-buddies/
[150] https://www.researchgate.net/publication/333339073_Hotspot_Analysis_Iranian_cyber-activities_in_the_context_of_regional_rivalries_and_international_tensions
[151] https://www.forbes.com/sites/claudiarosett/2014/12/12/north-korea-and-iran-partners-in-cyber-warfare/?sh=db0b1f559aa7
[152] http://www.thetower.org/article/how-iran-and-north-korea-became-cyber-terror-buddies/
[153] https://theiranproject.com/blog/2016/04/06/russia-china-greatest-cyberthreats-iran-growing/

5. Targets

Two categories of targets can be distinguished. On the one hand, Iranian hackers can attack foreign targets. It is noteworthy that the Iranian cyber-attacks are thoroughly correlated to the geopolitical context. Such logical is not observable in China or Russia where cyber-attacks are separated from the geopolitical context in the physical world. Moreover, the Iranian cyber-attacks are characterized by the massive presence of external destructive operations (sabotage). Russia and China prefer to use these operations for intelligence or information warfare purposes.

Iran is often depicted by Western countries as an aggressor and the major responsible for the cyber-attacks. However, such actions should be understood in a wider geopolitical context. In February 2020, American forces killed in an operation at the Baghdad's airport Qassem Soleimani, the head of the Iranian Quds forces and the head of the Iraqi PMF, Abu Mahdi al-Muhandis. This operation spurred wide demonstrations against the American military presence in the Middle East in Iraq and Iran. Israeli intelligence was reportedly helping the American forces in the operation against the two leaders by providing their geolocation.[154]This action that followed the withdrawal of the U.S. from the JCPOA triggered a dramatic increase of tensions between the U.S. and Iran which can degenerate into overt conflict. To answer this crisis, the U.S. adopted the maximum pressure policy against the Iranian regime, hoping that the increase of the economic pressure against its population would degrade the Iranian power and lead to the collapse of the regime.[155] This strategy is mainly based on economic sanctions but also on large scale cyber-attacks although there is no publicly declared strategy regarding the cyberspace on the American side.

Iran is often depicted by Western countries as an aggressor and the major responsible for the cyber-attacks. However, such actions should be understood in a wider geopolitical context.

The Iranian military strategy hinges very often on defensive and second-strike capabilities. Very often, offensive actions from Iran are correlated to a previous damaging attack or perceived offensive from its enemies. Michael Eisenstadt conveyed this rationale into tit for tat logic.[156] For its external operation, Iranian hackers are operating with the same rationale. Cyber operations are perfect for the Iranian government to strike its enemies and to use this destructive potential as leverage in potential negotiations with the U.S. Moreover, Western experts highlighted that the implementation of the JCPOA was correlated with a drop of the Iranian destructive cyber-attacks abroad.[157] These attacks resumed almost immediately

[154] https://www.i24news.tv/fr/actu/israel/diplomatie-defense/1578810565-les-renseignements-israeliens-ont-contribue-a-eliminer-soleimani-nbc-news

[155] https://ecfr.eu/publication/reviving_the_revolutionaries_how_trumps_maximum_pressure_is_shifting_iran s/

[156] https://www.washingtoninstitute.org/policy-analysis/irans-lengthening-cyber-shadow

[157] https://moderndiplomacy.eu/2019/11/27/usa-iran-cyber-war-part-of-hybrid-war/

after the withdrawal of the U.S. from the nuclear deal and are increasing with the new imposition of sanctions by the U.S.

Therefore, the Iranian regime uses cyber offensive operations to retaliate against attacks from its adversaries. Iranian hackers don't have always the opportunity to target high-level institutions and officials in countries with very efficient cyber protections. Iran may be tempted to attack soft targets or a third country which is a regional ally of its enemies and with less sophisticated cyber capabilities. Universities, some private companies, NGOS, military and diplomatic staff, media, or unprotected critical infrastructures are for example the ideal targets when their digital protection is not ensured.

However, Iranian hackers can sometimes launch cyber offensives for intelligence purposes. The Iranian regime is still isolated on the international stage and needs to improve its industrial capabilities to maintain its economies, particularly in the defence sector, aerospace industry, extractive industry and telecom firms. Iranian hackers have targeted some Western companies specialized in these fields to get information from their database. "There is an evolution underway within Iranian-based hacker groups that coincides with Iran's efforts at controlling political dissent and expanding its offensive cyber capabilities," reported Nart Villeneuve, senior threat intelligence researcher at FireEye.[158] "We have witnessed not just growing activity on the part of Iranian-based threat actors but also a transition to cyber-espionage tactics. We no longer see these actors conducting attacks to simply spread their message, instead choosing to conduct detailed reconnaissance and control targets' machines for longer-term initiatives."

On the other hand, Iranian hackers also attack internal targets and have a different strategy. At the internal level, cyber-attacks serve mainly for intelligence and information warfare. The toolset available to Iranian hackers are more efficient for this purpose.

6. Current cyber confrontations

Saudi Arabia

Saudi Arabia seems to be the most targeted country by the Iranian cyber-attacks. The country suffered from wide-scale cyber offensives from Iran. These attacks were successful due to the lack of digital protection implemented by Saudi companies.[159] According to Recorded Future, Iran would cash in from this vulnerability to launch cyber strikes to retaliate against the first strike from another more powerful country.[160] Some international experts also highlighted that Iran could use the weaknesses of the Saudi cybersphere to test the efficiency of its malware before launching other attacks against Israel or the U.S.[161]

[158] https://moderndiplomacy.eu/2019/11/27/usa-iran-cyber-war-part-of-hybrid-war/
[159] https://potomacinstitute.org/divisions/36-science-and-technology-policy/cyber-readiness/cyber-readiness-translations/105-kingdom-of-saudi-arabia-cyber-readiness-at-a-glance
[160] https://www.fifthdomain.com/home/2017/02/07/irans-cyber-strategy-a-case-study-in-saudi-arabia/
[161] https://www.fifthdomain.com/home/2017/02/07/irans-cyber-strategy-a-case-study-in-saudi-arabia/

Moreover, the current relations between Saudi Arabia and Iran are particularly tense due to the current political rivalry between the two countries and due to the proxy war in Yemen and Syria. The Iranian regime may be tempted to use increasingly this tool of hybrid warfare to destabilize Saudi Arabia and to hit its civilian infrastructures.

> Some international experts also highlighted that Iran could use the weaknesses of the Saudi cybersphere to test the efficiency of its malware before launching other attacks against Israel or the U.S.

In 2012, Iranian hackers launched the Shamoun attack in the framework of the operation Cleaver against the Aramco and the RasGas (Qatar) oil facilities.[162] The attack occurred during Eid holidays, at a moment when most of the employees were absent. This malware was created to erase the list of files from the system, rendering the computers unusable. An infected computer can also spread the malware to other computers of the network. The virus destroyed around 35,000 computers from the Saudi company, representing a loss of ¾ of the Aramco's computers. The attack was not harmful for oil production but it severely jeopardized the shipping contracts with foreign customers.[163] According to international experts, 10 million dollars and 5 months were necessary to recover from this attack and to protect the network of the firm. The Iranian hacker group "cutting sword of justice" claimed its responsibility for that attack and justified it by the damaging actions led by Saudi Arabia in Syria and Bahrain at that time. The attack was launched in the wake of the cyber-attack against the Iranian Kharg oil terminal. According to international experts, this attack would have been led to retaliate against the resuming of sanctions against the Iranian regime imposed by Obama's administration.

The Shamoun attack was followed by other malware attacks against the King Faysal foundation, the Saudi Stock exchange, Human rights organizations, the Saudi Minister of defence and various companies.

To protect from these offensives, the first national security strategy was launched in 2013 by the Saudi government. In 2017, the National Cyber Security Centre was created and incorporated as a branch of the Ministry of Interior. Qatar and the UAE followed the very same path of digital protection.

In 2016 and 2017, the Shamoun 2.0 malware resurfaced in Saudi Arabia to destroy different databases from the Saud Central bank, private sectors, general authority aviation, the Ministry of Labour and extraction companies. The attack was justified by the actions led by the Saudi coalition in Yemen and Syria and the religious tensions with Iran with the execution of the Shia cleric Sheikh Nimr al-Nimr, accused of terrorist offences.[164] The offensive was accompanied by photos of the civilians killed during these conflicts. The virus disappeared again before resurfacing in 2018 as a new version which targeted critical Saudi infrastructures such as oil, energy, and telecommunication grids.

[162] https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html
[163] https://www.theregister.com/2012/08/29/saudi_aramco_malware_attack_analysis
[164] https://www.bbc.com/news/world-middle-east-35213244

Saudi Arabia does not retaliate and attack Iran with direct cyber and kinetic operations. Aside from the cyber offensive, Iran numerously targeted Saudi Arabia through the use of missiles through its Houthis proxies and directly. The Aramco facilities were once again targeted in September 2019 in a drone and missile attack from Iran.[165] This bold offensive never met any repercussions from the Saudi side. Several experts suspect that Saudi Arabia uses its relations with other countries, as proxies, to retaliate against Iran.

Israel

According to Amos Yadlin, the former Israeli military intelligence director, and the incumbent head of the Institute for National Security Studies, Iran and Israel are currently confronting in a tense cyber conflict.[166] Previous Israeli intelligence operations endeavoured to stop the nuclear progress of Iran and tried to hamper the regime to obtain a bomb. Israeli intelligence units (particularly the famous Unit 8200, specialized in SIGINT) actively participated in the design and launch of the Stuxnet attack against Iran.[167] Israeli operations also targeted Iranian nuclear scientists directly.

Israel developed very sophisticated cyber capabilities and a comprehensive intelligence strategy to employ these tools. The concept of wars between wars developed in parallel the Israeli defence industry which becomes dramatically performant in cyber espionage and sabotage.[168] Israeli intelligence and electronic warfare was the cornerstone of the Israeli tactical capabilities and first developed during the wars against Hezbollah. These capabilities were further developed on the Syrian ground. During the Operation outside the Box in 2007, Israeli jet fighters evaded the Russian radars placed on the Syrian ground by the manipulation of enemies' sensors.

Iranian hackers cannot compete with the Israeli level in cyber defence.[169] Prime Minister Netanyahu tried to put the cyber industry at the top of the Israeli defence agenda and launch massive plans of investment in this sector.[170] 125 million dollars were invested in the development of cybersecurity. The Israeli government also foster the training of young students from the age of 13 to the use of Internet tools with the Tsahal (Israeli Army). Under his authority, the Israeli National Cyber was created in 2011.

Israeli intelligence units (particularly the famous Unit 8200, specialized in SIGINT) actively participated in the design and launch of the Stuxnet attack against Iran.

[165] https://www.csis.org/analysis/iran-yemen-and-strikes-saudi-arabia-changing-nature-warfare
[166] https://www.insurancejournal.com/news/international/2020/05/29/570415.htm
[167] https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fworld%2fnational-security%2fstuxnet-was-work-of-us-and-israeli-experts-officials-say%2f2012%2f06%2f01%2fgJQAlnEy6U_story.html
[168] https://besacenter.org/perspectives-papers/israel-intelligence-factory/
[169] https://www.jigsawacademy.com/why-the-israelis-lead-the-world-in-cyber-security-expertise/
[170] https://www.infosecurity-magazine.com/news/netanyahu-boasts-of-israels-cyber-1/

Israel has also specific units dedicated to cyber operation such as unit 8200 and Hahaz. These bodies are specialised in electromagnetic information and cryptography. Unit 8200 is included in the IDF and specialized in SIGINT, cyber and technics research. Some experts estimate that it is composed of about 5, 000 active members with reservists who serve at least 3 weeks per year. Unit 8200 allegedly collaborated with CIA to launch the Operation Olympic Games against Iran. Kaspersky Lab suspects this Unit to bet at the origin of the Duqu malware that stroke Iranian and European targets.

Iranian hackers tried to challenge the Israeli forces on the cyber theatre of confrontation.[171] In 2015, Iranian hackers launched a large cyber-attack against Israeli telecom companies, media outlets, universities, and national security offices, members of diplomatic staff and members of the Knesset. From 2015, the Israeli government answered through the creation of the National cyber authority which aims at creating cyber clusters to train more cyber experts in Beersheba valley to increase the strengths of the Israeli cyber defence.[172] This plan was particularly efficient. From 2016, Israel hosts more than 300 cyber companies representing 20% of the world's private cyber sector.

However, Israeli superiority has not impeded the continuation of Iranian attacks. In May 2016, the Iranian APT Oilrig launched a cyber offensive against a website server and infected more than 120 Israeli institutions.[173] Iranian hackers also launched DDOS attacks against the sole Israeli company which provides telecom infrastructures in the country. These attacks were easily repelled by Israeli forces but demonstrated the determination of Iranian hackers. Moreover, since 2017 Iranian hackers regularly attacked electric grids and water facilities in Israel.

The last Iranian attack could be remoted to the offensive against the SCADA system of the Israeli Water authority on April 25, 2019.[174] According to Reuters, the attack aimed at impacting the chlorine control pump operation installations, through the denied access to the interface. This attack constituted a real red flag for the Israeli government since it targeted directly a civilian facility. The attack was allegedly led to retaliate against the actions of Israel against Iranian and Hezbollah's positions in Syria. The Iranian government probably intended to hit directly Israel while it also aimed at keeping sufficient deniability. The strike was efficiently repelled by Israeli forces. However, its success could have triggered a massive sanitary crisis in the country which was suffering from a severe drought amid the coronavirus crisis. Israeli cybersecurity firms identified the Jerusalem Electronic Army as the potential source of the attack.[175] The group is a Palestinian threat actor linked to the Gaza Cyber Gang. It previously claimed its responsibility for the penetration into the Israeli military services. The Iranian government has never admitted the responsibility for this attack.

[171] https://www.aspistrategist.org.au/israel-and-iran-cyber-winter-is-coming/
[172] https://russiancouncil.ru/cyberiran
[173] https://spacewatch.global/2017/05/iranian-linked-oilrig-hacker-group-accused-cyber-espionage-operation-israel/
[174] https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/
[175] https://www.zdnet.com/article/israel-says-hackers-are-targeting-its-water-supply-and-treatment-utilities/

However, the correlation between the geopolitical context and the interests of the Iranian regime let believe Israeli cyber experts, that the actions were supported by the Iranian elites.

On May 9, 2020, the Washington Post reported a wide cyber-attack against the Shahid Rajee port located in Bandar Abbas in Iran.[176] The attack reportedly paralyzed its economic activities for a week. The port is crucial for the Iranian economy. 60% of the Iranian trade is exported through this port and Iran imports 85% of its whole goods through these facilities. The Iranian government tried to downsize the scale of the attack. However, experts estimated that the offensive was retaliation from the Israeli side for the attacks launched by the Iranian hackers.[177] The answer could be found disproportionate regarding the scope and the consequences of the Iranian attack against the Israeli water facilities. The offensive seems to occur to re-establish a balance of power advantageous to the Israeli side. However, a report from the Atlantic Council described this event as separated from the previous attacks against the Israeli Water authority.[178] According to this source, the scope and the force of the attack indicate a long-term operation and could not be prepared shortly. The operation could have been a counter proliferation attack aiming at reducing the import and exports of sensitive components for the Iranian weapon systems from this sensitive location.

Iranian hackers tried to retaliate against Israel. On May 21, 2020, an amateurish intrusion was launched against Israeli company websites.[179] The offensive led to the defacement of 300 websites from firms, political groups, organizations, individuals. Israeli experts could not state that the attack was orchestrated by the Iranian government but Iranian hackers were designated as the authors for this offensive. The disruption intervened on the Quds day in Iran, a day symbolically important for the Islamic regime which is marked by anti-Israeli and anti-American demonstrations.

The confrontation between the two states is still ongoing. On July 2, 2020, an explosion occurred on the upper level of the centrifuge in the Natanz nuclear facility. The explosion destroyed the centrifuges which were designed to speed up the enrichment of uranium and were suspected to be used in the building of weapon-grade nuclear material. The centrifuges could work up to 8 times faster than usual centrifuges. Iranian regime suspects the intervention of a new Israeli cyber-attack against the Iranian centrifuges. This information was not confirmed on the Israeli side. Moreover, intelligence experts think that the incident was more probably triggered by a direct explosion rather a cyber-attack on the nuclear facility.[180] Israeli powers could have launched this operation. Regional countries fear that the end of the JCPOA would lead Iran to the resuming of its military nuclear program which could destabilize the whole region. A series of blasts in Iranian facilities were also reported

[176] https://www.al-monitor.com/originals/2020/05/israel-us-iran-mike-pompeo-aviv-kochavi-cyberattack-port.html
[177] https://www.al-monitor.com/originals/2020/05/israel-iran-syria-amos-yadlin-cyberattack-port-water-system.html?emailaddress=justinemazonier%40gmail.com
[178] https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/
[179] https://www.timesofisrael.com/israeli-websites-hacked-in-cyberattack-be-ready-for-a-big-surprise/
[180] https://www.reuters.com/article/us-iran-nuclear-natanz/iran-threatens-retaliation-after-what-it-calls-possible-cyber-attack-on-nuclear-site-idUSKBN2441VY

recently. Just before the attack against the Natanz nuclear facility, the missile factory in Parchin exploded as well as a Hospital in the area of Tehran. Later, Fabian Hinz, an independent OSINT analyst, reported an explosion in the petrochemical plant in Mashahr and the Sahid Bakai industrial group.[181] The pipeline in the city of Ahvaz in Isfahan also exploded recently. The Iranian government accused Israel of these attacks. None intelligence experts could confirm this information and whether these explosions were due to cyber-attacks.

The United States

The U.S. was also under the threats of the Iranian cyber- attacks. The biggest one launched by Iranian hackers was the operation Ababil, which hit the American financial sector in 2012.[182] The group Iz Ad Din al Qassam noticed the beginning of their operation on the website Pastebin.com on September 18, 2012. The operation was launched in 3 series of attacks (the last one was carried out in 2017). 1,000 websites from American banks were attacked by a DDOS operation which rendered impossible the transactions on online platforms. The U.S. Bancorp, J.P. Morgan Chase, Bank of America, PNC Financial Services and SunTrust Bank were attacked. American banks were obliged to invest 10 million dollars to palliate these vulnerabilities.

According to some experts, this attack would have been launched to protest against the broadcast of the film the Innocence of Muslims, whose trailer was revealed on YouTube. The attack could have been also retaliation against the American sanctions imposed on Iran. According to cybersecurity experts, this attack would have occurred to retaliate against the American sanctions against Iran which rejected this country form the international SWIFT monetary transfer system.[183] This attack was one of the most destructive cyber-attack launched against the U.S.. The group Izz ad-Din Qassam claimed the responsibility for these actions. In 2016, the U.S. Department of Justice indicted 7 Iranian hackers (identified as Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, Omid Ghaffarinia, Sina Keissar and Nader Saedi) for their participation in the operation and the attack against 46 institutional targets. In 2013, this APT is suspected of having breached a dam in Bowman Avenue near Rye Brook in New York. The incident was first reported by the Wall Street journal.[184] The attack was not very sophisticated but Iranian hackers achieved to control the flood gates of the dam. In 2016, the U.S. Department of Justice identified and accused 3 members from the Iranian Sun Army APT and some Iranian companies (such as the IT security team and the Mersad Company for having carried out this attack.

[181] https://www.timesofisrael.com/gantz-on-iran-blasts-not-every-event-that-happens-there-is-connected-to-us/

[182] https://www.timesofisrael.com/gantz-on-iran-blasts-not-every-event-that-happens-there-is-connected-to-us/

[183] https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html

[184] https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

In 2013, Sheldon Adelson, the CEO of Sands Corporation, was interviewed regarding the American negotiations with Iran on the nuclear deal (JCPOA).[185] During this interview, he said that the U.S. should attack Iran with a nuclear weapon in its deserts and avoid any negotiations. "You want to be wiped out? Go ahead and take a tough position," Adelson stated.

In retaliation against these accusations, Iranian hackers launched in February 2014 a malware attack against the servers of the Las Vegas Corporation's computers. Three-quarters of the servers of the Casino were wasted. 40 million dollars were needed to repair the damages caused.

Between 2012 and 2014, Iranian hackers launched the widest cyberattack ever organized by Iranian perpetrators. 40 organizations among 16 countries were targeted. This attack was a rare example of external intelligence attack carried out by Iranian hackers. During the first phase of the operation codenamed Cleaver by international experts, Iranian hackers achieved to penetrate the U.S. Marine intranet through a malware attack.[186] Between October 2013 and April 2014, Iranian hackers targeted American defence companies in an operation codenamed Saffron Rose.[187] This attack specifically targeted aerospace and defence companies. Iranian defence industries could have stolen information from these entities through their database to develop its own technologies. According to the security company FireEye, the Ajax security Team or Rocket Kitten APT could be at the origin of this operation. According to CrowdStrike, the APT Flying Kitten could also be the perpetrator. The operation would have been carried out with the use of specifically designed malware and phishing operations to obtain email accounts from the victims. "It is unclear whether the Ajax Security Team operates in isolation or if they are a part of a larger coordinated effort on the part of the Iranian government," FireEye said.[188] "The team itself uses malware tools that, based on FireEye research, do not appear to be publicly available or in use by any other threat groups. Although we have not observed the Ajax Security Team using zero-day attacks as a means to infect victims, members of the Ajax Security Team have previously used publicly available exploit code in website defacement operations."

Between 2012 and 2014, Iranian hackers launched the widest cyberattack ever organized by Iranian perpetrators. 40 organizations among 16 countries were targeted. This attack was a rare example of external intelligence attack carried out by Iranian hackers.

[185] https://www.bloomberg.com/tosv2.html?vid=&uuid=ed855540-695f-11eb-b4f9-654f42c26827&url=L25Id3MvYXJ0aWNsZXMvMjAxNC0xMi0xMS9pcmFuaWFuLWhhY2tIcnMtaGl0LXNoZWxkb24tYWRlbHNvbnMtc2FuZHMtY2FzaW5vLWluLWxhcy12ZWdhcw==

[186] https://www.csoonline.com/article/2854686/cylance-unveils-details-of-iran-based-hacking-in-operation-cleaver-report.html

[187] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

[188] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

American assets were targeted through different operations carried out from Iran and targeting various actors across the West and the Middle East. The operation Wilted Tulip, launched in 2017 targeted various academics, governmental entities, organizations and companies in these zones. The operation APT 33 between 2016 and 2017 attacked aerospace companies in the U.S. and extractive companies in Saudi Arabia.

In 2018, the CIA obtained wider prerogatives from the American government to launch a cyber offensive.[189] From that date, the CIA does not need to obtain anymore the consent from the National Security Council, a civilian monitoring body, to check the legality of their actions on cyber operations. This former requirement avoided the total freedom for the intelligence service to conduct some damaging attacks against foreign targets whose links with a government was not proven (such as charities, NGOs). According to Yahoo News, more or less 12 operations were already launched in the world and targeted in majority Iran, Russia and North Korea. According to this media outlet, the CIA revealed in 2019 the hacking tools of APT 34 on a Telegram channel. The personal data of IRGC intelligence agents and information of 15 million credit cards from Iranian banks would have been spread by the CIA on a Telegram channel.

According to FireEye and Crowd Strike, cyber warfare between the U.S. and Iran is still ongoing. In June 2019, American President Donald Trump announced new sanctions against Iranian petrochemical industries.[190] This announcement was followed by the downing of an American RQ-4A Global Hawk High-Altitude drone by Iranian forces on June 20, 2019.[191] According to Iranian forces, the American surveillance drone would have violated the Iranian airspace. The IRGC affirmed that it achieved to shot down the drone. This event can refer to the downing of the American RQ-170 Sentinel in 2011 through electromagnetic warfare.[192] In return, American forces have triggered an offensive cyber strike against the IRGC rocket and missile control launchers, targeting the Command and Control System of the body.[193] This event highlighted the Iranian potential to increase its intelligence capabilities through the extension of SIGINT and electronic warfare. These capabilities could help Iran to develop its intelligence collection capabilities and erode the potential electronic-warfare measures. Iran developed extensively its defensive equipment such as modern command and control systems and military-satellite jammers and radars systems. Iran can extend its capabilities to obtain data on its adversaries through these new equipment's and the decrease the reliance of Iran on its extensive cyber capabilities.

[189] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf
[190] https://www.nytimes.com/2020/10/26/world/middleeast/trump-sanctions-iran-oil.html
[191] https://time.com/5611222/rq-4-global-hawk-iran-shot-down/
[192] https://time.com/5611222/rq-4-global-hawk-iran-shot-down/
[193] https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fworld%2fnational-security%2fwith-trumps-approval-pentagon-launched-cyber-strikes-against-iran%2f2019%2f06%2f22%2f250d3740-950d-11e9-b570-6416efdc0803_story.html

7. Internal targets

Iranian cyber tools are more effective against internal targets. Iranian hackers usually hit political opponents, corporations, NGOs, internal corporations as well as ethical and religious minorities. Governmental institutions can also be attacked due to the heterogeneity nature of the Iranian regime and the climate of suspicion present among different entities of the Iranian elites. Very often, the Basij Cyber Council and some APT (the Iranian Cyber Army, the Sun Army, Magic and Rocket Kitten are the entities that monitor the use of the cyber space by the population.[194] These entities are also engaged in information warfare and propaganda in the cyber space.

Iranian hackers usually hit political opponents, corporations, NGOs, internal corporations as well as ethical and religious minorities.

Governmental and private hackers can trace different Telegram users and to reach them through this communication app and arrest suspected users.

State representatives from the moderate government of Rouhani were particularly targeted. According to Anderson and Sadjapour, Magic Kitten would have achieved to penetrate and steal the Iranian Government Expediency Council, which is headed by Rouhani.[195] Several spear-phishing attacks were attempted against the civil servants who worked in the negotiation team for the JCPOA. These attacks would have been performed by the IRGC. The Ministry of Foreign Affairs would have been suffering from such attacks as well as Abdolrasool Dorri Esfahan, a Canadian-Iranian member of its nuclear negotiating team, who was arrested in 2016 under accusations of spying.[196] The accounts of the Iranian Ministry of Foreign affairs would have been targeted by a defacement campaign on social media and several thefts of emails data which compromised sensitive information on the Rouhani government.

Independent media were concerned also by censorship and cyber-attacks. Jason Rezaian, a Washington Post correspondent in Iran was arrested by the IRGC in July 2014, after having suffered from a cyber-attack against his Gmail account, allegedly led by Flying Kitten.[197]

Several Shia religious establishments were hit as well, particularly in Qom which hosts the Centre for Science of Islam Seminaries.[198] Religious minorities are more threatened. Bahai members were accused of conspiracy against the Iranian government and suffered from numerous cyber defacement attacks against its websites.[199] Cultural organizations, artists

[194] https://russiancouncil.ru/cyberiran
[195] https://russiancouncil.ru/cyberiran
[196] https://www.arabnews.com/node/1174421/middle-east
[197] https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fworld%2firan-confirms-arrest-of-post-correspondent%2f2014%2f07%2f25%2f54fdbc9c-13f6-11e4-8936-26932bcfd6ed_story.html
[198] https://www.article19.org/ttn-iran-november-shutdown/
[199] https://carnegieendowment.org/2018/01/04/iran-s-internal-targets-pub-75142

and satirists that do not fit the ideologies of the regime are potential victims for Iranian hackers. Finally, Iranian hacking groups targeted terrorist groups such as the ISIS and other Sunni jihadist organizations; the Baluchi Sunni and the Kurdish organization were also regularly hit by Iranian cyber-attacks.

8. Vulnerabilities

8.1. Foreign targets weaknesses

Iranian hackers can displace the battlefield to civilian infrastructures anywhere in the globe. Iranian hackers are targeting in priority the weaknesses of their adversaries and the critical facilities are more and more digitalized. The American Department of Homeland Security (DHS) defines critical infrastructures as "the essential services that underpin American society and serve as the backbone of our nation's economy, security and health.[200] We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family." According to Security Info Watch, these infrastructures comprehend 16 categories such as "chemical, commercial facilities, communications, critical manufacturing, dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, transportation, waste and wastewater, and nuclear reactors, utilities and waste".[201]

These infrastructures, less protected than the military ones are considered as a soft belly for Iranian hackers. An attack against them can spur massive economic, sanitary and security problems in a society more and more relying on them. Hackers can for example control of the SCADA systems and deregulate the usual working of the facilities or steal critical information.

"Iran is very technically capable of attacking our critical infrastructures," reported Joe Weiss, a managing partner at Applied Control Solutions. [202]

These facilities are under protection even in the U.S., a country where cyber capabilities are developed. Dan Coats, Director of National Intelligence, expressed his concern regarding the lack of protection for the American facilities against cyberattacks. He reported in 2018: "The system was blinking red.[203] Here we are nearly two decades later and I'm here to say the warning lights are blinking red again." Iranian hackers tried to take control on the American dam in New York in 2013. In 2014, the FBI revealed that a Chinese hacker group named Ugly

[200] https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions
[201] https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions
[202] https://www.newsweek.com/cyber-attack-rye-dam-iran-441940
[203] https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions

Gorilla achieved to infiltrate the control systems of infrastructures in the U.S. According to the FBI, the Chinese hackers would have achieved to access to the control systems regulating the flow of gas.[204] In 2016, the cybersecurity company FireEye reported that there was no national cyber security plan to protect the American Department of Transportation.[205] Very often, the design of a security plan against cyber-attacks is decided at the lowest level, letting a wide window of opportunity for Iranian hackers.

Iran could also use the cybersphere on the military field against the United States. Iran could in the past destroy American drones through the use of electromagnetic warfare. With the development of new technologies on the battlefield and the emergence of the Internet of Battlefield Things (IOBT) and the use of the 5G, the U.S. and industrialized, militarized countries could be found vulnerable regarding the growing Iranian cyber capabilities.[206] Aircraft carriers, precision weapons, radars, drones, command and control centers can be targeted by cyber-attacks.

Iran could also use the cybersphere on the military field against the United States. Iran could in the past destroy American drones through the use of electromagnetic warfare.

The Gulf States are also very vulnerable regarding the cyber threats against their critical infrastructures. The increasing digitalization of critical infrastructure raised the interconnection between the cyber sphere and physical world. The UAE boasted its connected smart cities. Iran can impose very devastating consequences for the Gulf with remote means. Among the most sensitive targets, oil and extraction industries can be targeted but more particularly desalinisation plants which provide drinkable water to most cities in the Gulf region. For example, 43% of the world desalinization plants are located in Saudi Arabia.[207] In 2009, a leaked document from the U.S. state department stated that if the Ras al Khair plant, the largest desalinization plant in the world, located on the seashores would be closed or destroyed, Riyadh would be forced to evacuate its whole population within one week since the plant aliments in drinkable water the capital. According to cyber experts, Iranian forces could also attempt to create cyber-attacks against missile defence systems in the Gulf region and in Israel to avoid the detection of incoming missiles.[208] The Iranian ICA and Hezbollah's cyber unit allegedly attempted to attack the Israeli warning radars.

Iranian hackers have the potential to cause severe damage against critical civilian infrastructures.[209] In May 2016, Iranian hackers allegedly attacked the Turkish electricity network, causing a power failure in half of the country. This attack deprived from electricity

[204] https://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/?sh=3e7e11cf5f39
[205] https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html
[206] https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html
[207] https://www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation
[208] https://www.csis.org/analysis/irans-threat-saudi-critical-infrastructure-implications-us-iranian-escalation
[209] https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/

40 million of inhabitants for 12 hours. This attack was reportedly carried out to retaliate against the role of Turkey in the Syrian conflict.

It can be highlighted that there is a lack of cooperation among Gulf members and other states to implement efficient cybersecurity architecture against Iranian attacks. These threats are not extremely serious and can become anodyne due to their lack of sophistication if the targeted countries adopt integrated and comprehensive cyber defence approaches. However, the absence of such cooperation leaves windows of opportunity for Iranian hackers to attack soft targets and less protected countries. Thorough cooperation in cyber defence between Israel and Saudi Arabia for cyber defence and missile defence system could be particularly positive and avoid the current spillover situation.[210]

Such cooperation could be however particularly complicated to obtain. The Gulf region demonstrated its vulnerabilities regarding internal cyber-attacks that destabilized the political cooperation between states.[211] In 2017, the Qatari Tweeter account of the Emir Tamim bin Hamad Al Thani was hacked and displayed fake declarations on Iran, spurring a diplomatic crisis between the GCC members. The hackers reportedly used UAE based devices in Qatar to launch the attack against the Qatari News Agency websites to place fake comments from the Qatari Emir. The UAE always denied such allegations. This crisis which was a result of pre-existing simmering tensions between these states resulted in the division of the GCC countries. Iran could cash in from this situation to strengthen its cooperation with Qatar and Turkey and to challenge Saudi Arabia and the UAE. This division decreased the threat represented by a coalesced GCC against Iran. This event showed the vulnerability of the Gulf peninsula regarding cyber-attacks and informational warfare. It could create opportunities for the Iranian regime to divide more the GCC countries.

The third impediment would come from the absence of international and national control regarding Iranian cyber capabilities. There are no international laws regarding cyberwarfare and on the consequences of such attacks on the civilian and physical sphere, as the International Humanitarian Law regulates the jus in bellum in another theatre of war. At the internal level, Iran is not a democracy and can employ bolder techniques since the government does not need to be transparent with its population. This opacity increases the strength of the Iranian cyber warfare.

At the strategic level, the absence or weakness of the answers provided by Western powers under cyber-attacks could jeopardize the strategic balance between them and Iran. If any doubts are let regarding their capabilities to retaliate against the Iranian cyber offensives, the deterrence balance could be eroded in the long term.[212] According to Jason Healey, a demonstrative effect in cyber theatre (which he designated as a loud shout) is necessary to reach a sufficient deterrence effect. However, this visible cyber retaliation could backfire against the retaliating state. Indeed, cyber experts stated that Iranian hackers managed to learn from the Stuxnet virus to build their own malware and launch cyber-attacks. The U.S.

[210] https://moderndiplomacy.eu/2020/12/23/israeli-gulf-cyber-cooperation/
[211] https://www.chathamhouse.org/2019/05/gulf-divided-impact-qatar-crisis
[212] https://www.washingtoninstitute.org/policy-analysis/irans-lengthening-cyber-shadow

fears that the extensive use of cyber weapons could legitimize its use by other actors and give the necessary tools indirectly and lead to an uncontrollable situation. Victim states should, therefore, adopt a more comprehensive cyber strategy and set up precise red lines against the Iranian cyber-attacks to avoid such situation and be obliged to use kinetic means of warfare, with the risk of escalation.

8.2. Iran`s vulnerabilities

The Iranian territory also offers different interesting targets for a potential cyber-attack from its enemies. The Latyan Dam, located on the Jajrood River, at 25 km from Tehran in the south of the city of Lavasan is the main source of water of the capital. A cyber-attack against this facility could potentially destroy the city. The Iranian economy is also dependent on the production of energy products and an offensive against these companies could be as damaging as for its enemies. Israel demonstrated with its attack against the Iranian port recently that the Iranian regime is not protected enough from these attacks and Western and regional enemies can easily challenge Iran on the cyber sphere. This logic could lead to the launch of cyber-attacks with physical consequences for the victim country. The Stuxnet strike was the best example for the Iranian regime to assess the destructive power of cyber operations. The latest Israeli offensive against the Iranian port demonstrates that Iranian hackers cannot drop the Iranian strategic moderation in its hybrid warfare without fearing escalation and retaliation. Very few reports are dealing with the offensive actions led by Western powers and Israel against Iran. According to the Iranian Minister of Foreign Affairs spokesperson, Abbas Mousavi, thousands of cyber-attacks would have been launched against Iranian infrastructures, mainly from the U.S. It is not, however, possible to check precisely the veracity of this information, but reports on the Iranian cyber vulnerabilities are lacking in the Western researches.

The latest Israeli offensive against the Iranian port demonstrates that Iranian hackers cannot drop the Iranian strategic moderation in its hybrid warfare without fearing escalation and retaliation.

The Iranian cyber capabilities can also be void regarding the pre-existing knowledge of the techniques used by its adversaries. Very often, Iranian hackers use old pirated versions of Western software that are not updated and leave vulnerabilities for the Iranian systems using it. Western adversaries are also protected against a potential attack by Iranian hackers using these tools.

The military issues become more complex if the retaliation is not epitomized in a digital form. In May 2019, IDF stroke Hamas' positions in retaliation of a cyber-attack.[213] The strike aimed at destroying a building where members of the APT HamasCyberHQ.exe were located. It was the first time that a kinetic strike was launched to retaliate against a cyber-attack. With the

[213] https://www.zdnet.fr/actualites/israel-repond-aux-attaques-informatiques-du-hamas-par-une-frappe-aerienne-39884331.htm

development of offensive cyber operations, this practice could be potentially imposed against Iranian hackers in the future.

Finally, the Iranian government demonstrated that it was particularly sensitive about any external interference into its internal information space. During the last demonstrations in November 2019, the Iranian government cut off the Internet access to 80 million people for several days.[214] Moreover, Iranian people keep on using Western and foreign communication apps.

Conclusions

'The supreme art of war is to subdue the enemy without fighting.' This quote from Sun Tzu could sum up the rationale behind the Iranian cyber warfare and its integration within its hybrid strategy. Cyberwarfare is included in the Iranian asymmetric and hybrid strategies and is used as a means to demonstrate the posture of the Islamic Republic on the international stage. The Iranian cyberwarfare is therefore heavily correlated to the geopolitical context and the variations of the Iranian relations with external countries impact the use of this tool.

As part of its hybrid strategy, Iran uses this tool of warfare to hide the State responsibility behind the Iranian cyber-attacks. Cyberwarfare creates confusion for the adversary and denies the possibility to retaliate at a low cost. The Iranian government created therefore a very complex cyber ecosystem composed of different layers of actors with a specific hierarchy. A digital network of proxies is also present at the internal and external level.

The intensity and nature of the Iranian cyber operations changes with the targets. The internal operations are more efficient against the population to control its activities in cyberspace and to limit the use of the Internet in its territory. At the internal level, the cybersphere is perceived as the main vulnerability for the control of the government on the population. The Iranian government is particularly sensitive to the threat from the free use of the Internet and communication app by its population as the Green Movement demonstrated in 2009. Specific actors are intended to control thoroughly the cyberspace at the internal level.

At the external level, the Iranian actors modulate their actions according to the level of sophistication of their adversaries and the nature of the confrontation on the physical world. The Stuxnet attack was the second milestone that shaped the Iranian cyber warfare and the organization of its external cyber operations. Iranian actors target principally less protected States in the Middle East with a low level of sophistication. However, the lack of technicity does not hamper Iranian hackers to cause great damages with sabotage operations by targeting sensitive civilian infrastructures. Gulf countries are particularly at risk regarding the lack of protection of the critical facilities. American, Israeli and European infrastructures are not better protected. The low coordination between a comprehensive state strategy and

[214] https://edition.cnn.com/2019/11/19/middleeast/iran-internet-shutdown-intl/index.html

the lowest level of the targeted facilities opens windows of opportunities for Iranian APT. The Ababil attack or the operation against the Turkish electric grids is a case in point of the level of harmfulness of the low-sophisticated level of Iranian attacks against carefully chosen targets. Iranian hackers also launch sabotage operations that increased in the wake of the ratification of the nuclear deal against civilian Western targets.

These trends could be exacerbated in the next few years with the increasing financial and geopolitical pressure against the Iranian regime. Cyber sabotage operations could become the new tool for the Iranian government to cause damages against its enemies at a minimal cost. The current cyber cooperation between Israel and the Gulf States could however shift this trend and impose a strategic balance with Iranian hackers on the cyberspace.

Topchubashov Center
Globus Center, Floor 7,
609 Jafar Jabbarli Str.
Baku AZ1065, Azerbaijan

info@top-center.com
www.top-center.com


@Topcenterorg


@topchubashovcenter


Topchubashov Center