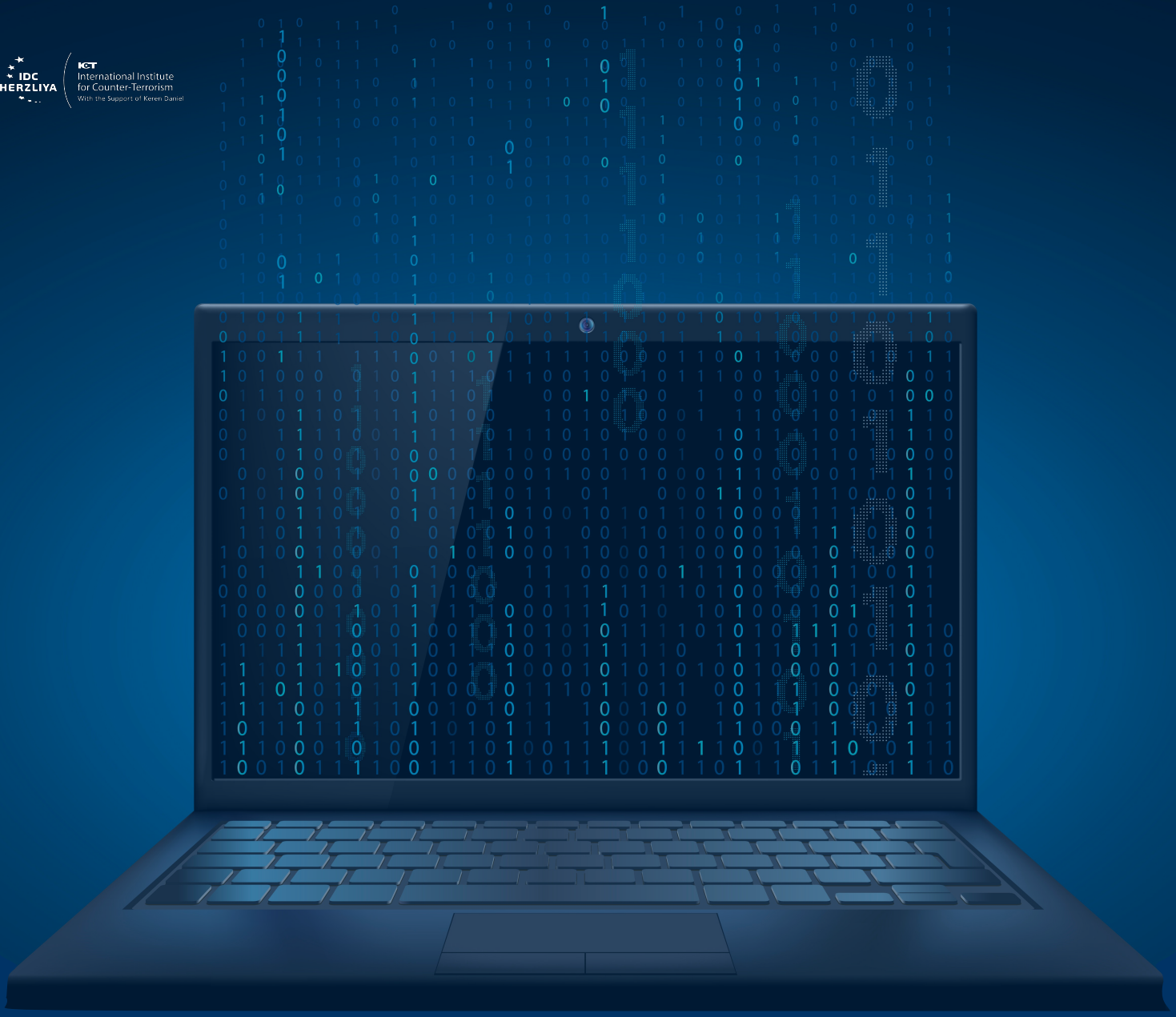
IDC HERZLIYA
ICT International Institute for Counter-Terrorism
With the Support of Keren Daniel



IRGC Cyber-Warfare Capabilities

Giacomo Spadoni

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy.

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT ICT CYBER-DESK

The Cyber Desk Review is a periodic report and analysis that addresses two main subjects: cyber-terrorism (offensive, defensive, and the media, and the main topics of jihadist discourse) and cyber-crime, whenever and wherever it is linked to jihad (funding, methods of attack).

The Cyber Desk Review addresses the growing significance that cyberspace plays as a battlefield in current and future conflicts, as shown in the recent increase in cyber-attacks on political targets, crucial infrastructure, and the Web sites of commercial corporations

Table of Contents

Introduction: The Cyber-Domain as a Level Playing Field 4
Iran's Cyber Doctrine 4
Cyber-Warfare Institutions in Iran 6
Official Cyber-Institutions 6
Unofficial IRGC Hacking Teams 7
Life and Behavior of Iranian Hackers 11
Tactics, Tools and Targets of IRGC Cyber-Campaigns 12
Social Engineering and Espionage 12
DDoS Campaigns 13
Malware/Virus Campaigns 13
Phishing Campaigns 14
Complex Cyber-Attack: Operation Saffron Rose 14
Operational Military Practice of Iranian Cyberwarfare 15
Cyber Operations Finalized to the Geolocalization and Acquisition of Order of Battle of Enemy Forces 15
Military Industrial Espionage 15
Attacking Critical Infrastructure 16
Policy Solutions 16
References 20

Introduction: The Cyber-Domain as a Level Playing Field

The cyber domain is composed of cellular technologies, space-based communications, and intranets, in addition to the internet of networked computers. Cyberspace often has a physical infrastructure layer which is dictated by the financial laws of rival capitals along with partisan laws of control and self-governing jurisdiction. It also sports a virtual, also referred to as an information layer, which is characterized by increasing commercial proceeds to scale as well as political exercises which often make jurisdictional governance difficult. Costs are usually law in the informational realm. As such, attacks can be flung from here against the corporeal domain in which capitals are quite expensive and scarce. The control of the corporeal layer can have both extraterritorial and territorial consequences on the information layer. In turn, cyber power can construct the intended results within and outside infobahn.[1]

It is noted that the blockades to entry in the virtual domain are noticeably low. Consequently, non-state players and small nations get to play major roles at very low heights of cost. While comparing land, sea, and air, *"cyber stakes three physiognomies with the land fare, factoring in three key aspects namely the number of players, an opportunity for concealment and ease of entry. Notably, on land, ascendency is not a ungrudgingly achievable benchmark."* (Nye, 2011).

The Future of Power describes the dispersion of power as one of the inordinate power shifts of the era. Cyberspace serves as an excellent exemplar of this larger trend where the biggest powers are highly unlikely to rule this domain as much as they have done with space, air or sea. They might have grander resources, but this is also accompanied by greater susceptibilities. At this specific stage in the elaboration of the machinery, offense tends to dominant protection in cyberspace. Some of the major countries on the globe namely the U.S, China, France, Russia and Britain have a sizable aptitude than other official and non-official actors. However, it makes minute sense to have a conversation regarding dominance in cyberspace. Thus, since the cyber-encryption field is a level playing field, major powers do not enjoy a technological superiority compared to non-state actors or states sponsors of terrorism. Iranian programmers have the same knowledge, capabilities and means of their American, Israeli or europeans counterparts. The threat coming from Iranian cyber-operations is more real than ever (Nye, 2011).

Iran's Cyber Doctrine

Currently, the Islamic Republic of Iran is guided by three primary features including dominant leaders, a powerful military organization and a strong national cultural identity. These are considered as important aspects in the strategic development of the nation, while also playing a critical role as important receptors for strategic targeting. One other prominent factor that is playing a critical role in the development of Iran's cyber activities is its hostility towards Israel. It is noted that the Arab-Israeli conflict has been central to modern-time politics in the Arab world and has shaped the region, not just politically but also economically and socially. Iran has grown to find this conflict beneficial for its role in the region as the nation at the forefront of bashing Israel.

[1] The information superhighway

Iran's cyber policies have been significantly influenced by the country's history as a major civilization and hegemonic regional power. As such, Iran plans to further capitalize on its influence in the region to further these policies and make them work for the benefit of the nation and its people. In recent times, this has seen Iran execute cyber-attacks targeted towards its regional adversaries in a move that many have criticized and cited that it might lead to a series of cyber-attacks, all to the detriment of the Iranian Citizens. To minimize the risk, Iran has opted to procure the services of armed proxies and partners to further its agenda and cyber-attacks towards its adversaries (Eisenstadt, 2016).

In the Iran's warfare strategy, the cyberspace is a component of the country's doctrine of asymmetrical warfare. Cyberwarfare, is seen as a tool that could help the country like to fill the gap with the superior Conventional military capabilities of its rival countries (U.S., Israel, Saudi Arabia) along with other classical asymmetrical strategy such as terrorism and guerrilla warfare. Iran, especially IRGC, believes that enhancing its cyberwarfare capabilities could have, at least partial deterrence against its enemies. Iran will likely recur to all its cyberwarfare capabilities against enemy countries, in cases of serious diplomatic or military escalation with the hope do deter its enemy from further attacks.

As a means to defend itself, Iran has come up with two main goals. One of the goals is to create what it refers to as a "technological envelope" which will protect all the country's critical infrastructure and sensitive information against cyber-attacks. Iranian learned the lesson from the Stuxnet experience. The virus was responsible for damaging the Iranian uranium enrichment program which took the country significantly back. The second goal is to stop and foul all cyberspace activities by its opposition elements and persons who oppose the regime. To these individuals, cyberspace serves as a key platform for communication, distribution of information and the organizing of anti-regime activities. As such, by thwarting all their cyberspace activities, their objectives would not be achieved. The Iranian government has a program to create a separate, independent communications network that is important in the achievement of the goals mentioned above (Martins, 2018).

It is noted that Iran's success in using cyber strategies to quell domestic dissent came to be the foundation for the further development of cyber capabilities and strategies. In the recent past, the country identified and adopted cyber warfare as an effective addition to its arsenal. This is a country whose leadership began toying around with the use and application of cyber warfare as a deterrence weapon, not just against foreign threats to the regime, but also local threats as well. It also explored the tech and utilized it as a way to spy on foreign nations and familiarizing itself with their activities. As such, both offensive and defensive aspects were followed as Iran used cyber sabotage and espionage tactics.

Iran's tactic involves a web of individuals informally allied to the IRGC and the Iranian administration. It is a type of ideologically allied middle administration made up of people who are not only faithful to the management but also demonstrate adequate religious duty. This made up the medium tier which converted intelligence urgencies into segmented virtual tasks which would later be auctioned out to multiple contractors. There were times when the contractors would compete with each other, whereas in other instances, they would work together. However, payment was only made once the objectives were achieved. Consequently, a quasi-capitalistic objective was achieved in the end — a system that pitted contractors against each other, all so that they could have influence within the Iranian government (Gundert, 2018).

Cyber-Warfare Institutions in Iran

Official Cyber-Institutions

Iran system of cyber-agencies is complex and comprises of various governmental military and civilian bodies, in additions to a considerable number of proxies groups, which are formally independents from the Islamic Republic but operates under IRGC or Ministry of intelligence supervisions.

History has proven that cyber operations targeting Iranians and originating from Iran arise out of nowhere, conduct campaigns for ambiguous reasons over a short timeframe, then disappear. The Iranian agenda to create a distinct and self-governing communications grid, therefore, proves integral in this context. Currently, the highest government body that is responsible for dealing with cyberspace issues is a founded body by the name High Council of Cyberspace. This outfit was set up back in March of 2012 on the orders of Ayatollah Khamenei. The primary objective was to institute high-level dogmas on the infobahn. Following the instituting of this body, all other Iranian officialdoms in control of cyber actions within the country were committed to the implementation of the policies which this body instituted. Notably, the body was comprised of the top-level Iranian personalities like the president, the heads of jurisdictional power as well as the legislature. Other notable figures included the head of the government-run media stations, the commander-in-chief of the IRGC and the constabularies, the ministers of information, science, telecommunication, and culture, among others. Inside this body IRGC is the key player.

A central organization is the Cyber Defense Command (Gharargahe Defa-e Saiberi), an organism that has a primary defensive role in the Iranian Cyberwarfare Doctrine (Carnegie Endowment for peace, 2018).

The body is composed mainly by military personnel and is under the supervision of the General Staff of the Armed Forces. The main goal of this cyber-agency is to defend the country against cyber-attacks and develop strategies against cyberspace threats. Additionally, another body with defensive orientation the MAHER Information Security Center, which operates under the authority of the communications and information technology ministry. The agency' primary role is the emergency first response in case of cyber attacks. Another Iranian cyber-unit is the Committee for Identifying Unauthorized Sites and FATA, that act as cyber-police. Its tasks involve the dealing with internet and the monitoring of Iranian internet usage (Masharof, 2018).

Given the role of the IRGC with regards to military leadership and the framework associated with that, it's duties extend to the supervision of cyber operations both externally and internally. Also, notably, Iran's use and adoption of outsourcing allow the country to maintain a safe distance that grants them deniability about its involvement. The use of proxies has always proven to be highly effective in the maintenance of plausible deniability.

This paper will focus mainly on the activitivity of IRGC. and its associates/contractors. Associated with IRGC. there are different cyberwarfare-units. The Revolutionary Guards established The Basij, the Basij Cyberspace Council with functions of production of pro-Iranian propaganda and offensive hacking tasks. In addition to "official" cyber institutions, there are some hacker groups that are used as a "front organizations", deeply connected with IRGC and Iranian Intelligence apparatus.

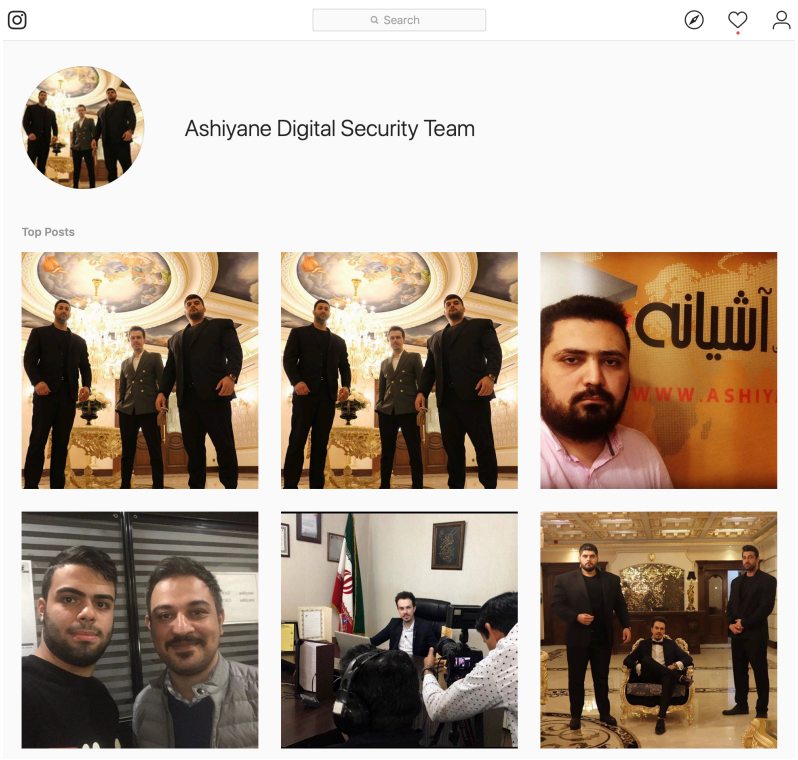
UNOFFICIAL IRGC HACKING TEAMS

Ashiyane Digital Security Team

A prominent hacker group linked to the Revolutionary Guards is the Ashiyane Digital Security Team. It is believed that in 2010, the group hacked, in a two days major operations, 1,000 important websites in the UK, the US, and France (Masharof, 2013).

Kamalian, the head of the hacker group, mentioned that in recent years, Ashiyane was responsible for hacking hundreds of sites, comprising one that was compered in Denmark. This was all in answer to the publication of caricatures that depicted the Prophet Muhammad, the use of "Arabian Gulf" in place of the "Persian Gulf", along with the good old reprisal for cyber-attacks on sites that belonged to Ayatollahs Ali Sistani and Makarem Shirazi. Kamalian further pointed out that the group was also responsible for the hacking of tens of Israeli sites back in 2006 throughout the Lebanon war and in 2009 during Operation Cast Lead in Gaza.

Kamalian further pointed out that as of 2010, his group operated independently and spontaneously. However, he acknowledged that it also cooperated with the Iranian military apparatus in the development and improvement of security. He noted that many countries were waging cyberwars since this type of war was and still is more meaningful regarding time, cost and forfeiture of life. As such, he reiterated that the planet's most commanding governments such as the United States, Iran, China, and Russia ought to have organized groups for cyber warfare. To his defense, he stressed that his team always functioned in the context of the goals established by the government and faith, noting that the team has never conducted projects that went against or were targeted towards the Iranian country and its people (Masharof, 2013).

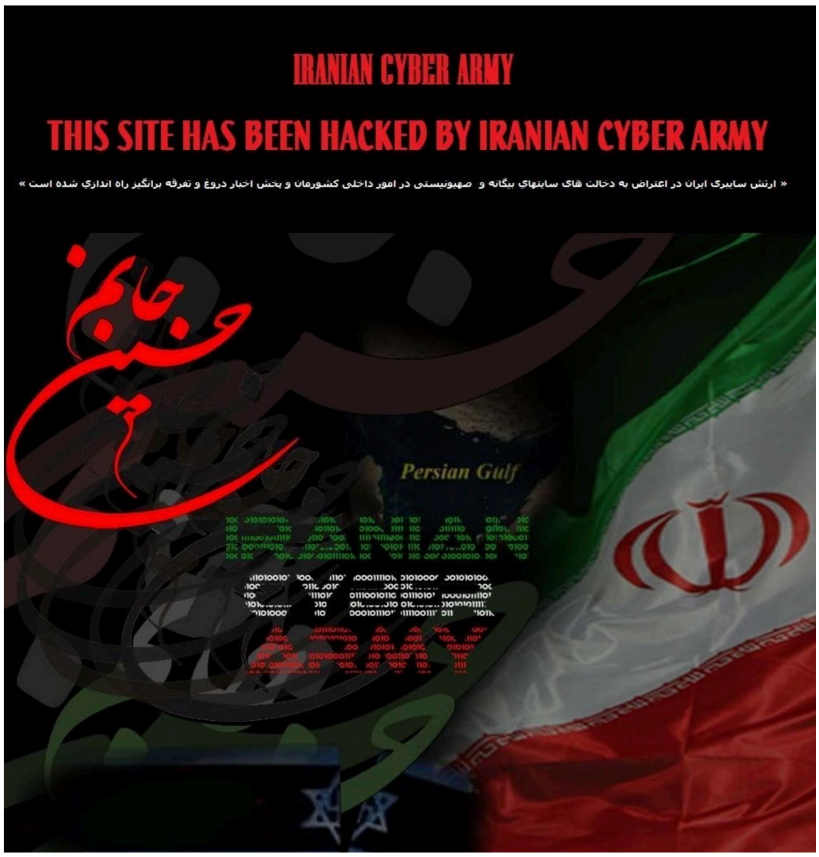


A screenshot of the Instagram page of Ashiyane Digital Security Team

Iranian Cyber Army

Another organization, known as Iranian Cyber Army, defaced twitter in 2009 as a response to the widespread use of the social network in the organization of popular revolts following the June 2009 elections in Iran, shutting down the service for more than two hours. The group is also responsible for the defacement of many important websites associated with Iran's political opposition, Israeli companies, non-aligned Persian-language media, social media platforms, posting pro-government message. In February 2011, Khamenei's representative in the IRGC, Ali Saeedi, revelead that the Iranian Cyber Army was operating on behalf of the IRGC (globalsecurity.org, 2018).

It is noted that the activity of Iran's cyber army is believed to be directly overseen by a specific IRGC Intelligence unit. In Ebrahim Jabbari, commander of the Ali Ebn-e Abi Taleb Guards in Qom 2010, claimed that the outfit was the second-biggest cyber army in the world (Masharof, 2013).



A screenshot of defaced website. Source: the deep web closed forum Irananonymous

Mabna Institute

The IRGC outsourced cyber operations also to The Mabna Institute, an organization that was founded in 2013 to assist Iranian universities and scientific and research organizations in obtaining access scientific resources outside the country. In 2016, the organization carried out cyber intrusions networks belonging to at least 320 universities based in 21 countries, among them, United States, Australia, Canada, China, Germany, Ireland, Israel, Italy, Japan, Malaysia, the Netherlands, Norway, Poland. The group stole credentials of Professors, students's data and confidential research materials In addition, the attackers stole employee e-mail accounts at nearly 50 private companies around the world (Gundert, 2018).

Wanted by the FBI poster of individuals affiliated to the Mabna Institute. Source: FBI, 2018

Cyberspace Research Institute of Iran's

The Cyberspace Research Institute of Iran's (CSRI) is a research center affiliated with the prestigious Shahid Beheshti university in Iran. Direct system connectivity between Spanish and Iranian establishments shows that they either have a deep scholastic relationship which entails sharing information with one another, or the sizeable transfer of records and info from these Spanish institutions is undeserved. Scholars have been keen to point out that it is highly implausible that CSRI would have a valid commercial interest in Spanish administration departments. As such, the large section of data conveyed between the two entities over a diminutive period is a clear pointer of possible malevolent activity (Gundert, 2018).

ITSecTeam and MERSAD

Back in 24th March 2016, a grand bench in New York indicted a total of seven Iranian nationals who were hired by two Iran-based IT corporations- ITSecTeam (ITSEC) and Mersad Company (MERSAD). These two companies had a history of performing work for the Iranian administration, including the Islamic Revolutionary Guard Corps. The two Iranian nationals were charged with hacking, along with their involvement in an extensively distributed denial of service (DDoS) attack campaign that lasted for over 176 days (United States Department of Justice, 2016).

The DDoS attack was targeted at 46 preys, primarily those in the U.S monetary sector. Timing was between late 2011 and mid-2013. The perpetrators included Ahmad Fathi, 37, Sina Keissar, 25, Amin Shokohi, 25, Hamid Firoozi, 34, Nader Saedi, 26, Sadegh Ahmadzadegan, 23, Turk Server, 26 and Omid Ghaffarinia, 25. The occurrences disabled the victims' bank sites, preventing clients from opening their bank accounts on the web, and ultimately costing the dupes millions of dollars in costs that went into mitigating and neutralizing attacks on the servers. Firoozi was later charged with gaining unauthorized admission into the Supervisory Control and Data Acquisition (SCADA) systems of Bowman Dam which is situated in Rye, New York. He acquired access in August and September of 2013.

Virtual Anonymous Jihad

In June of 2013, Shirin Ebadi, an Iranian human entitlements avant-garde and Nobel laureate publicized that a hacker group by the name "Virtual Anonymous Jihad" which claimed accountability for several assaults on sites outside Iran, was run and directed by Iranian administration members.

Earlier on February of the same year, the same group had hacked and shut down the websites www.banisadr.org and www.enghelabe-eslami.com which were both linked to former Iranian leader and challenger to the regime — Abu Al-Hassan Bani Sadr. Sadr is currently in émigré in France. On March of the same year, the same group hacked www.mef.edu.sa a website that belonged to the Saudi Ministry for Higher Education. This was a move in remonstration against Saudi Arabia's engrossment in the Bahraini régime's ongoing subdual of Shi'ite protest in Bahrain. Later, in May, the group hewed www.lrtv.com a website that belonged to an Iranian oppositionist TV which operated in the United States. On top of that, they attacked a Facebook page which belonged to a BBC Farsi journalist by the name Siavash Ardalan.

Fast forward to June 13th, a day before the Iran top-level elections, the group again lacerated and shut down key regime challenger websites which functioned outside Iran. Among those hacked included www.ostanban.com, www.digraban.com and www.khodnevis.org. the group would later post messages such as "*To those who talk baloney, and to the legionnaires of the outsiders, there is no secure place. Anywhere you are, we are within scope of Hezbollah forces*" (Masharof, 2013).

Tarh Andishan/Ajax

The Iranian hacker team has since been dubbed Tarh Andishan/Ajax which loosely translated means "thinkers" or "innovators." The name came from traced OP blocks which registered to an entity by the name Tarh Andishan in Tehran. During their string of attacks, scholars noted that the group achieved complete access to airport gates, allowing them to spoof gate credentials. They further gained access to Go Daddy and PayPal credentials, allowing them to make fraudulent purchases on top of unfettered access to the victims' domains. Tarh Andishan made use of common SQL injection, watering hole attacks and spear phishing to gain admission to one or more workstations belonging to an aimed institute. They then used the privilege intensification feats and other useful tools to compromise supplementary systems and move further into the company's network (Constantin, 2017).

Charming Kitten

Charming Kitten is another group that was primarily linked to Iranian cyberespionage. It has been operating since 2014 and was responsible for a string of attacks with a specific focus on the field of academic research, media and human rights. Most of Charming Kitten's targets included individuals living in the United States, Israel, Iran, and the UK. However, there were victims in other countries including Switzerland, India, Germany, and France among others. Recently, this group made a move to hack accounts of US government officials to no avail. They have tried to gain access into private mails of nuclear technologists and US approvals officials. All this is according to data collected by Certfa, a London-based cybersecurity group. Charming Kitten has, however, not slowed down its advances. On numerous occasions, it has targeted private emails of more than 12 US Treasury officials, key figures in the enforcement of the nuclear deal between Tehran and Washington, along with Arab atomic scientists and Iranian civil society figures (Clearskysec.com, 2018).

Life and Behavior of Iranian Hackers

In the Islamic Republic, as is the case almost everywhere else, influence attracts safety and affluence. However, it also attracts a fabricated sense of safety, which is why contractors learn to work the game with sufficient surface-level devotion to the regime's philosophy. This is usually a move to gain provisional reprieves from misgiving long enough to be given work by the administration. The Iranian government values ideology more than skills. It is a move that allows the ruling elite to avoid defections and traitors.

Insikt noted that the Iranian administration contractors are often required to mine closed-trust groups. This is all in a bid to retain the best offensive cyber talent and to retain it for the longest time possible. The link that exists between the contractors and the forums indicate that the trust groups begin with the Iranian safety forums. Iranian hackers are also very highly educated, most of them having Ph.Ds. and Master's Degrees in

physics, mathematics and/or computer science. This is a totally different case compared to hacking crews in Europe or the United States. It is also noted that most Iranian hackers frequently attend schools in the West. Take Yashar Shahinzadeh, for instance, he is currently seeking a Master's Degree in information security at a prominent university in the UK (Bardin, 2016).

The morphing of an amateur hacker into a contractor for state security agencies is reflected in basic qualities and patterns of life found cross most threat actors. It is noted that there are clear indications that the threat actors documented are primarily Iranians, all operating within Iranian borders, unlike diaspora Iranians or non-Iranians. Their patterns are usually normal, just like any other office worker. They are active during the Iranian workweek and dormant during holidays. One thing to note, however, is that these individuals often lack professionalism. Additionally, they have a complete disregard for operational security due to insulation from the repercussions that follow their professionalism, or lack thereof. As such, the disclosure of their real names and aliases is very easy. One thing that makes them work with the government, however, regardless of their lack of professionalism, is their ideology. However, there are some disparities among such hacker groups, with some participants promoting the use of narcotics and the trade of pornographic material on social media, while some of their counterparts might be devoutly religious, staunch Muslims (Balvin, 2016).

Tactics, Tools and Targets of IRGC Cyber-Campaigns

Social Engineering and Espionage

IRGC program in recent years has invested substantial efforts in its social engineering and psychological program. The aim of IRGC social engineering attacks are double: *psychological warfare and the acquisition of strategic information from enemy targets*. IRGC enables its strategy by using tier hacker groups, as it is normal for the group. These groups have been using different tactics of social engineering.

IRGC front companies are developing spyware-enabled apps for cyber-surveillance and repression. Moreover, groups supervised by IRGC have created mobile apps marketplaces similar to Apple Store and Google play in order to distribute spyware-enabled apps. Additionally, some of these apps are available also on the cited mainstream marketplaces, potentially exposing millions of users worldwide to the IRGC's spyware and surveillance, although the main target are Iranian citizens. Through these app stores IRGC has diffused messaging apps alternative to the popular telegram (which counts about 40 millions users in Iran). The various Iranian cyber units uses these apps to track and combat the spread of anti-regime information (Carnegie endowment for peace, 2018).

Some hackers thought to be operating with the Iranian administration, in the recent past, satirized a young female photojournalist on social media. This went on for over a year, and they leveraged people's ignorance to lure men employed in industries tactically important to Tehran's local adversaries. The impersonated photographer was Mia Ash, and her persona was active on various sites including Blogger, LinkedIn, WhatsApp and Facebook. What this revealed was a social contriving plot by Iran to entangle its targets with a "honey pot," a typical spying trap that usually involves seduction, a tool mostly used by scandalous hackers (Voltz, 2018).

Twitter and Facebook are among the few platforms that announced the deletion of hundreds of social media accounts that showed suspicious activities. The two companies stated that these accounts were linked to a systematic Iranian disinformation campaign abroad. In typical fashion, the groups associated with the campaign presented themselves as independent outlets when, in fact, they were Iranian state media. Their content was packaged in such a way that it pushed narratives and issues that were solely in line with Iranian foreign policy. These included anti-Saudi, pro-Palestinian and anti-Israeli themes, along with USpolicies that were favorable to Iran (Tabatabai, 2016).

In late 2016, Khawaja Asif who was the then Pakistani minister for defense, took to Twitter to threaten Israel with nuclear war. The post would later be deleted, but it stemmed from a post that Asif had come across online about the Israeli defense minister himself threatening nuclear war against Pakistan. The website from which he got the information from was AWD News which turned out to be part of a social media and fake news campaign out of Iran (Michel, 2018).

Charming Kitten, a hacking group mentioned earlier, also established a media outlet dubbed "The British News Agency". Its purpose was to lure targets through a campaign that targeted academic research media outlets and political advisors with a focus on Iran. This, in turn, drove Iran into a sprawling disinformation operation on Facebook where hundreds of thousands of people within and outside the country were targeted. This campaign started as far back as 2011, with hundreds of accounts on Facebook and Instagram being used to promote the false agenda and propaganda on which people with ill intent rode on. Massive disinformation was targeted at individuals in Latin America, the United States, and the Middle East among other locations. The aggressiveness in these campaigns grew with every passing year as was reported by Facebook officials (Kirk, 2014).

DDoS Campaigns

The primary cybersecurity tactic used by Iranians was launching a DDoS attack, with the intention of overloading websites of countries which they considered to be hostile. Between late 2011 and mid-2013, the Iranian cyber army was responsible for the take-down of both private and government websites in various sectors including the banking and business sectors. They had traversed borders, with victims being as far as the United States. There was an operation dubbed "Ababil" by the group "Izz ad-Din al-Qassam Cyber Fighters." It was active from September of 2012 through to October of the same year. It targeted American financial institutions and banks, with the same DDoS attack strategy. According to the hacker group, the operation was a revenge attack for an anti-Islam film which was uploaded to the internet in which it purportedly insulted the prophet, Muhammad. Some of the companies whose websites were taken down included Wells Fargo, PNC and Bank of America. (Fixler, 2018).

Malware/Virus Campaigns

IRGC associated groups have been recurring for years to the use malware and virus to attack network sand databases and commit data deletion of entity considered close the Iran's enemies. The most famous example is the cyber Iran's cyber attacks of August 2012 on the computers of the Saudi Arabian oil company Aramco and the Qatari gas company RasGas. The cyber-offensive was carried out thanks to the spreading of a computer virus called Shamoon, which was infiltrated through company servers and destroyed information

stored in them. A group called the Cutting Sword of Justice took responsibility for the attack by claiming that it was directed to the main source of income of Saudi Arabia, which was accused of committing war crimes in Bahrain and Syria (Globalsecurity.org).

Following the initial Shamoon attacks in 2012, a variant of the original malware was used in an attack against Saudi Arabia in November of 2016. Shamoon would later be blamed for destroying computers are at least six Saudi organizations that month, including the Saudi Aviation Regulator. The most memorable happening in the attack was the overwriting of files with an image of a 3-year old Syrian emigrant lying lifeless on a beach. That month, according to a Saudi state-run television, Al Ekhbariya, 15 government agencies were hit by Shamoon 2. The malware took control of the computers' boot records, preventing the PCs from being turned back on (Gundert, 2018).

PHISHING CAMPAIGNS

The already mentioned Mabna Institute was behind the large spearphishing campaign that targeted the e-mail accounts and computer systems of universities, private sector, international government organizations (such as UN) and companies of 21 countries. In the case of the academic institutions, victim professors and university personnel received malicious mails and fell in the trap believing they were dealing with colleagues who had expressed an interest in academic articles.

Many to clicked on links that recorded their credentials when they signed into what they thought were their secure university domains but were actually bogus sites controlled by the hackers. The Iranians stole data across all fields of research and academic disciplines, including science and technology.

With this complex phishing operation the institute successfully compromised approximately 8,000 of professors' accounts around the world. The campaign continued begin in April 2016 and finished in December 2017. According to estimates Iranian obtained for free material that would $3.4 billion to procure (Carnegie Endownment for Peace, 2016).

COMPLEX CYBER-ATTACK: OPERATION SAFFRON ROSE

IRGC has been proven capable to carry out complex operations which combines multiple type of cyber-attacks. FireEye researchers noted that the Ajax Security Team used a combination of phishing emails, fake login pages, and custom-built malware to get a hold of login credentials and other sensitive data. In one attack, the group responsible targeted a US-based aerospace company by creating a fake registration page for the 2104 IEEE Aerospace Conference. This followed emails to employees of the targeted company, prompting them to register for the conference. When the recipients followed the links in the email, they would be prompted to download software claiming to be a proxy required to gain access to the site. This "proxy software" was malicious which functioned in the same way as a Trojan horse. Once the target installed the program, the stealer would run another program called IntelRS.exe, thereby snooping on infected computers using various methods including taking screenshots, keylogging and gathering useful info such as hostnames, IP addresses and installed applications among others. On top of that, login credentials and cookies would also be collected as well (Villeneuve, 2013).

Operational Military Practice of Iranian Cyberwarfare

Operational military of cyber-attacks are variate, especially in the case of asymmetrical conflicts where the weaker actor can exploit the cyber-space to its own advantage. A cyberspace attack may be employed with the aim to deceive, degrade, destroy, and disrupt enemy or to acquire precious military intelligence. Since the cyber-realm is a level playing field, IRGC does not need a huge amount of financing and technological resources in order to create damage to other actors. In fact, even the hacking of a device belonging to a military official through a simple phishing attack has the possibility to cause a lot of disruption.

Cyber Operations Finalized to the Geolocalization and Acquisition of Order of Battle of Enemy Forces

Iranian hackers could be employed in order to track down enemy's capabilities in war theatres in the Middle east, where American, Europeans and Israelis have a presence.

Hackers could geolocalize enemy soldiers and extract information from personal devices and social network accounts using OSINT tools or through social engineering operations. In 2014 a selfie posted by soldier serving in Russia's 76th Airborne regiment with geotagging feature actived enabled the online OSINT organisation Bellingcat to discover that as many as 40 Russian troops had been killed in the Donbass war in Eastern Ukraine and thereby confirm the presence of Russian forces in the conflict, officially denied by the Russian government (Bellingcat, 2014).

In 2017, sensitive information about the location and staffing of military bases and spy outposts around the world were leaked by a fitness tracking company called Strava (The Verge, 2018).

The company released a data visualization map that showed all the activity tracked by users of its app, which allows individuals to track their exercise routines and share it with other users.

The graph showed all the activities ever uploaded to the app, with trillions of GPS data points. Strava can be run on smartphones and fitness trackers like Fitbit and its social features allow users to spot discover the most popular running routes in major cities, or spot people in more isolated areas who have atypical exercise patterns.

Military Industrial Espionage

IRGC could employ hackers in order to steal secret weapons projects, military document from western contractors. Iran has both the know-how and financial resources to carry out such operations which does not involve high costs. Chinese hackers have already proven effective in military industrial espionage, targeting especially USdefense contractor through various type of cyber-attacks (mainly malware and phishing attack). In 2015, a leaked NSA document revealed that China obtained more than 50 terabytes from US Department of Defense (DOD) and contractor Lockheed Martin. Among the data obtained by the Chinese were included radar, secrets and engines from the new f-35 military aircraft (Gertz, 2014). The Chinese even obtained the "Flight Test Plan" for the jet written by a US defense engineer. It is believed that some design technological features of the F-35 were included by Beijing in the new Chinese stealth jet, the J-20. The hacked data could allow Chinese air defenses to easily target the American jets in case of a future conflict. While Iran does not

have the industrial capability of building such advanced jets, IRGC could extensively benefit from these classified information, both in a defense manner (considering also that much of IDF technology is American), both as a boost for its own military industry.

Attacking Critical Infrastructure

As already mentioned before, between August 28, 2013, and September 18, 2013, Iranian hackers launched repeated cyber-attacks against Bowman Avenue Dam in the State of New York. One of the hackers, Hamid FIROOZI repeatedly obtained unauthorized access to the SCADA systems of the Dam, in Rye, New York, which enabled him access information to sensitive information such as the water levels and temperature, and control panel of the sluice gate, which allow to manage water levels and flow rates.

While the hackers have been able to release water from behind the dam given his remote access, they didn't have the capability to do it because the sluice gate had been manually disconnected for maintenance at the time of the intrusion.

This attack, could be considered a "test"; meaning that the threat is real and authorities should be prepared future threats, especially in geopolitically trouble times. Employing cyber-weapons in order to attack Industrial Control System (ICS) is an hard but not unlikely task, especially if hackers have physical access to the target product or have logical access to the ICS: an attacker would compromise a system that connects to the ICS. This could be a vendor support computer, an engineer laptop, a USB drive, or an engineer system on the corporate network allowed to access the ICS (Peterson, 2015).

Moreover, an attacker learns about the process and determines how to destroy a physical component or subsystem that will take time to replace (Peterson, 2015). Thus, not only cyber-security measures should be enhanced but also the physical security of critical infrastructure should be strengthened. In western countries, especially in Europe, it is often easy to roughly access critical such type of infrastructure like a dams, plant powers because there are no sufficient physical security measures. Additionally, workers of the infrastructures such as engineers and technicians, are vulnerable to social engineering attacks aimed to the obtaining of sensitive information, as seen before.

Policy Solutions

When approaching to the IRGC and more general, Iran cyber threat, different type of policies should be considered. Policies should take in consideration different aspects such as the cyber one, the political, diplomatic and military ones. The following are possible policy solutions suggested by the author:

1. Increasing Cooperation Bolster Information Sharing with US Allies to Improve Allied Defenses

As seen before Iran is a threat not only for declared "enemy countries" such as US, Israel or Saudi Arabia but also for neutral countries. Thus, greater cooperation among NATO members and other countries would protect the national interests of every country threaten by the IRGC threat. Information sharing between allies countries a better understanding of the Iranian cyber threat and facilitate the effectiveness of cyberspace defence.

A collective defense of countries threatened by the cyber-threat could develop in a cyber-security alliance on the style of NATO.

2. Dedicated Intelligence Units to Monitor Iran Cyber Activities

Countries threatened by aggressive Iranian behaviour on the Cyber-space should task the intelligence community to better analyze IRGC cyber investment, capabilities, industrial base, and actors.

Intelligence services need to examine regime's annual spending on cyber, IT technologies, project and infrastructures. Moreover, Iran technology imports and domestic production capacity should be deeply investigated. This would be extremely useful in order to prevent the Islamic regime from acquiring and importing military and dual-use technology necessary to improve IRGC cyberwarfare capabilities.

3. New Type of Sanctions

In 2014 President Obama, as a response to North Korea cyber-attack on Sony promulgated an Executive Order that barred ten individuals and three organizations, including North Korea's main intelligence agency and primary arms exporter, from accessing US financial systems. In reality, these sanctions only minimally affected the North Korea regime because it has been one of the most isolated countries in the world for a long time (Sanger, 2017). The actual economic sanctions on the Islamic Republic are not deterring IRGC from conducting cyber-attacks. There is a need of a different type of the sanctions. Effective sanctions should target individual and single group involved in cyber-operations, from the cyber-operators to the high echelon of IRGC an decision makers. It may therefore be effective to declare terrorists whoever is involved in cyber-operations and issue international warrants. Moreover, sanctioning groups and individual belonging to the revolutionary faction of the Islamic Republic would increase the probability of a internal rift with the republican institutions (such as government and the army) who are traditionally hostile to the roughly operations carried out by IRGC. Countries and international organizations could employ sanctions also a mean to deter foreign actors from providing indirect support to Iranian cyberwarfare operations. In fact, Iranians often use servers located outside or acquire apparently harmless IT services from abroad, which in reality are exploited for cyber operations. It is noted that strong relations between the Iranian regime and Russian Information security experts have shaped Iran's cyber activities in the recent past.[2]

4. Creation of International Cyber-Security Treaty

Countries who are threatened by Iran actions on the cyberspace should push in UN, G20 and other international bodies for the creation of a new worldwide treaty that will regulate cyber warfare activities. The new treaty should create an International cyber-security council. The Organization for the Prohibition of Chemical Weapons ("OPCW") would serve as an appropriate model. The OPCW is an independent international organization that was created by the Chemical Weapons Convention ("CWC"), a treaty that bans chemical weapons (Opcw.org). In order to effectively combat against state-sponsored cyber-attacks, the treaty should identify a clear and comprehensive definition of "state-sponsored cyber-attack. Additionally, it

[2] For example, see Shanghai Cooperation Organisation (SCO) The International Code of Conduct for Information Security.

should expressly authorize a punishment for state-sponsored cyber-attacks. The treaty would thereby deter states from committing these attacks and provide an effective remedy when they occur (Nye, 2015).

5. Deterrence by Denial with Cyber-Operations.

Until today Iranian cyber-attacks have gone often unpunished. Thus, Iranian actors gained confidence to act without consequences. No countries or entity has imposed deterrence costs on the Iranian rogue actors, with the most notably exception of Stuxnet, the Joint Israeli-American malware operation who effectively managed to destroy an Iranian nuclear centrifuge. Additionally, cyber operations are for their own nature more secretive than kinetic operations and is often difficult to attribute with precision the responsibility for an attack in the immediately aftermath. Military and intelligence agencies who confronts the Iranian cyber threat need to improve their capabilities for attack *attribution*. IRGC needs to know that if they carry out an attack there will be costs derived by retaliatory counter-attacks. Moreover, if a single country will be attacked in the future ally countries should cooperate in delivering a unified response in the cyber-realm. Stuxnet in this has been a milestone; the cooperation between United States and Israel resulted in strategic success. Deterrence is not the only solution to the IRGC cyber threat but it is essential to counter the menace. Deterrence by denial consist in imposing costs. Costs should be imposed with denial attacks (on form of DDOS, malware, phishing, ICS disruption) and with the strengthening of the cyber defense in order to deter attackers.

6. Improving Cyber-Defenses

Western Countries should improve the cyber readiness of both their private and public sector in order to prevent such type of disruptive attacks from foreign countries. The military and law enforcement personnel dedicated to cyber warfare and cyber-security should be increased.

Meanwhile some countries, such as Iran, Russia, China, North Korea have acquired some experience in the field of cyberwarfare; western countries (with the exception of Israel) have engaged a little in cyber-operations and are not ready for large cyber-ware scenarios.

The mentality of western militaries could be not adequate to the new threat of cyber-asymmetrical warfare. Many commanders see the using of a cyber-weapon as clear cut process, like conventional warfare and do not the cyber threat as a leveling field where enemies with less conventional power can overcome a biggest enemy.

In November 2016 the US Cyber command had only 1,000 men that were operational ready for cyberwarfare activities (Freedberg Jr, 2016). While it is true that cyber-soldiers are diluted also in other agencies (such as NSA), the number was inadequate if compared to US strategic needs. In March 2012, the IRGC claimed it had recruited around 120,000 personnel over the past three years to combat “a soft cyber war against Iran (The tower, 2015). While the claims are believed to be exaggerated, the human involved in the Iranian cyber-forces are estimated in tens of thousands. European countries find themselves even more unprepared to threat if compared with United states.

NATO countries must increase their funding in training for cyber-soldiers and setting up new units, considering also that the threats not only come from Iran but also from others rogue Cyber powers North Korea.

The private sector also should improve its cyber-readiness. More cyber-security experts are needed in the sector. Governments should support more cybersecurity programs in university and colleges. Moreover, it should facilitate an increasing integration and cooperation between the education system, the army and the private sector. The industry and the government should include sharing information and the exchange best practices.

Unlike conventional security issues, private individuals are more exposed to cyber-attacks due to the transnational and virtual nature of threats. This brings in more stakeholders, and increases the responsibility on individuals to protect themselves from crime and espionage. The burden to protect those users rests equally on governments and on the private sectors.

6. Securing Critical Infrastructure

It is imperative securing critical infrastructure (CI) in order to prevent effectively the cyber-threats posed by IRGC. Cyber-attacks on critical infrastructures, and the technology that enable it, have the potential for catastrophic nation, region or worldwide-ranging effects. Therefore, physical and cybersecurity of CI must be a top priority. In spite of, the great risk to critical infrastructure, the protection of industrial control system is not considered a relevant investment area. Companies do not perceive the risks adequately because profits from infrastructure cannot adequately quantified. The private sector must do its part. However, in matters of national security it’s the state that has to lead. Therefore, if private actors do not adequately perceive the risks governments and lawmakers must enforce it hoc legislature that require adequate standard of cyber-protection and with incentives and sensibilization campaign on the issue.

References

Joseph S. Nye, Jr. (2011) The Future of Power. Public Affairs.

Bardin, J. (2016) What it's like to be an hacker in Iran. Business Insider. https://www.businessinsider.com/what-its-like-to-be-a-hacker-in-iran-2016-2?IR=T

Duggan, P. M. (2015). Strategic Development of Special Warfare in Cyberspace. *Joint Force Quarterly*, *79*(4).

Eisenstadt, M. (2016). *Iran's Lengthening Cyber Shadow*. Washington Institute for Near East Policy.

Green, J. A. (Ed.). (2015). Cyber warfare: a multidisciplinary analysis. Routledge.

Jordan, T. P. (2016). The Law of Armed Conflict, Unconventional Warfare, and Cyber Attacks. *Nat'l Sec. L. Brief*, *6*, 37.

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128.

Leccisotti, F. Z., Chiesa, R., & De Nicolo, D. (2016). Analysis of possible future global scenarios in the field of cyber warfare: National cyber defense and cyber attack capabilities. In *Handbook of research on civil society and national security in the era of cyber warfare* (pp. 181-204). IGI Global.

Lupovici, A. (2016). The "Attribution Problem" and the social construction of "Violence": Taking cyber deterrence literature a step forward. *International Studies Perspectives*, *17*(3), 322-342.

Martins, R. P. (2018). Punching Above Their Digital Weight: Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *8*(2), 32-46.

Pelton, J. N., & Singh, I. B. (2019). How Nations and Smart Cities Can Cope with Cyber-Terrorism and Warfare. In *Smart Cities of Today and Tomorrow* (pp. 185-201). Copernicus, Cham.

Sahu, S. K., Anand, A., Sharma, A., & Nautiyal, N. (2016, February). A review: Outrageous cyber warfare. In *Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on* (pp. 70-74). IEEE.

Flixer A., Ciffullo F. (2018) Menace Iran's Use of Cyber-Enabled Economic Warfare. Foundation For Defense of Democracy.

The Verge. (2018). *Strava's fitness tracker heat map reveals the location of military bases*. [online] Available at: https://www.theverge.com/2018/1/28/16942626/strava-fitness-tracker-heat-map-military-base-internet-of-things-geolocation.

Bellingcat, (2014) Revealed: Around 40 Russian Troops from Pskov Died in the Ukraine, Reinforcement Sent In Retrieved from https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinfo HYPERLINK "https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinforcement-sent-in/"r HYPERLINK "https://www.bellingcat.com/news/mena/2014/08/27/revealed-around-40-russian-troops-from-pskov-died-in-the-ukraine-reinforcement-sent-in/"cement-sent-in/

Gertz, B. (2014). *NSA Details Chinese Cyber Theft of F-35, Military Secrets*. [online] Washington Free Beacon. Available at: https://freebeacon.com/national-security/nsa-details-chinese-cyber-theft-of-f-35-military-secrets/.

S. Department of Justice, Press Release, "Manhattan USAttorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against USFinancial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities," March 24, 2016. (https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated)

Jr., J. F. (2016, November 08). US Army Races To Build New Cyber Corps. Retrieved from https://breakingdefense.com/2016/11/us-army-races-to-build-new-cyber-corps/

The Tower. (2015). Iran Has Built an Army of Cyber-Proxies - Retrieved from http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/

Schlein, T. (2018, April 16). The United States needs a Department of Cybersecurity. Retrieved from https://techcrunch.com/2018/04/16/the-united-states-needs-a-department-of-cybersecurity/

Waterman, S., & Waterman, S. (2018). Cyber Command lacks authorities, capabilities, Pentagon watchdog says - CyberScoop. Retrieved from https://www.cyberscoop.com/cyber-command-lacks-authorities-capabilities-pentagon-watchdog-says/

Shinkman, P. (2019). How the US stacks up against its digital adversaries. Retrieved from https://www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries

Organization for the prohibition of Chemical Weapons, official website. Retrieved from https://www.opcw.org/

Masharof, Y. (2013). IRGC Claims Iran Can Hack Enemy's Advanced Weapons Systems, MEMRI. Available at: https://www.memri.org/reports/irans-cyber-war-hackers-service-regime-irgc-claims-iran-can-hac0k-enemys-advanced-weapons.

Olsen, C. (2018). *An Introduction To The Implications Of Iran's Cyber Capabilities For The US*. [online] Medium. Available at: https://medium.com/@chrisolsen97/us-implications-of-irans-cyber-capabilities-c4f88d3e2745

Villeneuve, N., & Moran, N. (2013). Operation Saffron Rose, Retrieved from: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," Atlantic Council, July 29, 2013, Available at: http://www.atlanticcouncil.org/publications/issue-briefs/iran-how-a-third-tier-cyber-power-can-still-threaten-the-united-states.

Masharof, Y. (2013). Iran's Cyber War: Hackers In Service Of The Regime; IRGC Claims Iran Can Hack Enemy's Advanced Weapons Systems; Iranian Army Official: 'The Cyber Arena Is Actually The Arena Of The Hidden Imam'. Available at :https://www.memri.org/reports/irans-cyber-war-hackers-service-regime-irgc-claims-iran-can-hack-enemys-advanced-weapons

Globalsecurity.org. (2018) Iran cyber operations, , Available at: https://www.globalsecurity.org/intell/world/iran/irgc-cyber.htm

Siboni, G. (2013). *Iran's Cyber Warfare*. [online] Inss.org.il. Available at: http://www.inss.org.il/publication/irans-cyber-warfare/

Carnegie Endowment for International Peace. (2018). *Iran: Target and Perpetrator - Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. [online] Available at: https://carnegieendowment.org/2018/01/04/iran-target-and-perpetrator-pub-75139

Gundert, L. and Chohan, S. (2018). Iran's Hacker Hierachy exposed. Recorded Future Available at: https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf

Office of Public Affairs. (2016) *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against USFinancial Sector.* The United States Department of Justice. Available at:https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-c HYPERLINK "https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged"h HYPERLINK "https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged"arged

Constantin, L. (2017). Iranian hackers compromised airlines, airports, critical infrastructure companies. [online] PCWorld. Available at: https://www.pcworld.com/article/2854272/iranian-hackers-compromised-airlines-airports-critical-infrastructure-companies.html.

Clearskysec.com. (2018). Charming Kitten: Iranian Cyber Espionage Against Human Rights Activists, Academic Researchers and Media Outlets. [online] Available at https://www.clearskysec.com/charmingkitten/

ABC News. (2018). Iran-linked group hacks nuclear scientists, US sanctions officials. [online] Available at: https://www.abc.net.au/news/2018-12-14/group-says-iran-hackers-hunt-nuke-workers,-us/10618296

Bardin, J. (2016). What it's like to be a hacker in Iran. [online] Business Insider. Available at: https://www.businessinsider.com/what-its-like-to-be-a-hacker-in-iran-2016-2?IR=T.

Kirk, J. (2014). Iranian group created fake news organization as part of hacking campaign. [online] PC World. Available at: https://www.pcwo HYPERLINK "https://www.pcworld.idg.com.au/article/546295/iranian_group_created_fake_news_organization_part_"r HYPERLINK "https://www.pcworld.idg.com.au/article/546295/iranian_group_created_fake_news_organization_part_"ld.idg.com.au/article/546295/iranian_group_created_fake_news_organization_part_

Voltz, D. (2018). Iranian hackers used female 'honey pot' on social media to lure targets, finds new research. [online] The Independent. Available at: https://www.independent.co.uk/news/world/iran-hackers-honey-pot-social-media-female-mia-ash-facebook-whatsapp-linkedin-pupyrat-a7864256.html.

Tabatabai, A. (2016). A Brief History of Iranian Fake News. [online] Foreign Affairs. Available at: https://www.foreignaffairs.com/articles/middle-east/2018-08-24/brief-history-iranian-fake-news

Craig Timberg, Elizabeth Dwoskin, Tony Romm, and Ellen Nakashima, “Sprawling Iranian influence operation globalizes tech’s war on disinformation,” The Washington Post, August 21, 2018. (https://www.washingtonpost.com/technology/2018/08/21/

CTECH - www.calcalistech.com. (2018). *Iranian Hackers Have Set Up a News Outlet to Court Possible Targets, Security Firm Says*. [online] Available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3726650,00.ht HYPERLINK "https://www.calcalistech.com/ctech/articles/0,7340,L-3726650,00.html"m HYPERLINK "https://www.calcalistech.com/ctech/articles/0,7340,L-3726650,00.html"l

Michel, C. (2018). *Fake Iranian news site provoked Pakistan’s nuclear threat against Israel*. [online] Thinkprogress.org. Available at: https://thinkprogress.org/source-of-pakistani-nuclear-threat-against-israel-revealed-as-fake-iranian-news-site-75831c3c1880/.

Staff, T. (2016). *Pakistani officials chide defense minister for Israel nuclear threat*. [online] Timesofisrael.com. Available at: https://www.timesofisrael.com/pakistani-officials-chide-defense-minister-for-israel-nuclear-threat/.