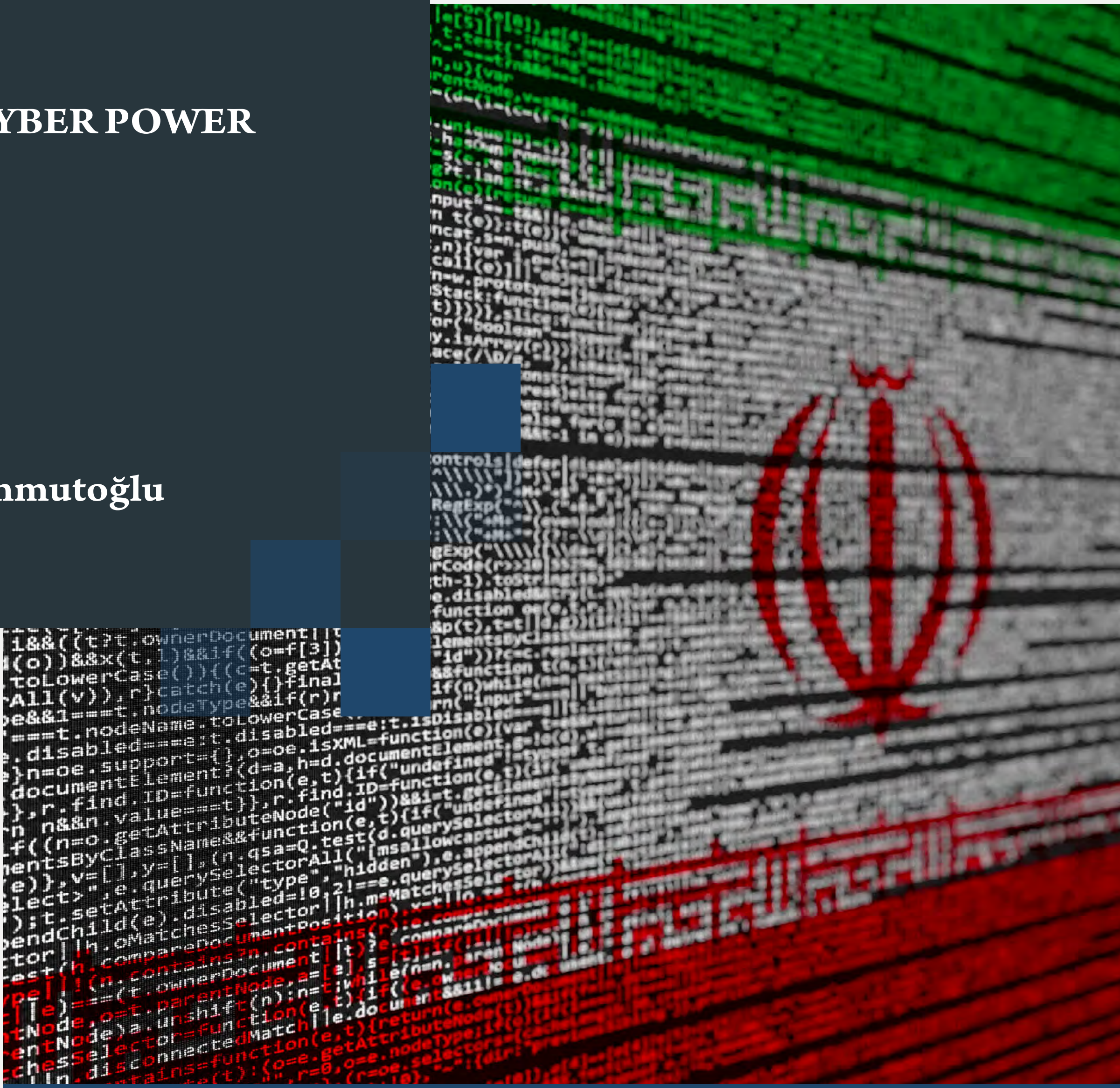
İRAM
YAYINLARI

IRAN’S CYBER POWER

Ersin Çahmutoğlu



Report

April 2021

İRAM
YAYINLARI

Editor in Chef : Dr. Turgay Şafak
Coordinator of Publications : Alper Tok

Editor : Saadat Eskandarifar
Layout : Hüseyin Kurt
ISBN : 978-605-7559-77-7

Center for Iranian Studies in Ankara
Ankara
Oğuzlar, 1397. St, No.: 14 06520 Çankaya, Ankara, Turkey
Phone: +90 (312) 284 55 02-03 | Fax: +90 (312) 284 55 04
e-posta: info@iramcenter.org | www.iramcenter.org
İstanbul
Üst Zeren St, No: 40 Levent, Beşiktaş, İstanbul, Turkey
Phone: +90 212 264 35 81 | +90 212 268 33 00 Fax: +90 212 264 35 18
e-mail: iramistanbul@iramcenter.org | www.iramcenter.org

İRAM
Center for Iranian Studies in Ankara

Iran's Cyber Power

İran'ın Siber Gücü

قدرت سایبری ایران

Ersin Çahmutoğlu

Ersin Çahmutoğlu graduated from National Defence University Strategy and Security Research master program after he defended his thesis "Cyberattacks as a Dimension of Hybrid Warfare and the Situation in Turkey". He has been working on cybersecurity for many years and has several publications in peer-reviewed magazines, on digital platforms, and in several books. He has specialized on the issues of the cyberweapon, state-sponsored cyber threat actors, and global cyber-espionage operations. The author continues his research currently in İRAM Security Studies.

İRAM
YAYINLARI

Report

Contents

Images

Abbrevıatıons

USA	: United States of America
APT	: Advanced Persistent Threat
UAE	: United Arab Emirates
CSJ	: Cutting Sword of Justice
DDoS	: Distributed Denial of Service
IRGC	: Islamic Revolutionary Guard Corps
ICA	: Iran Cyber Army
IHS	: Iran Hackers Sabotage
ISP	: Internet Service Provider
NIN	: National Information Network
NSA	: National Security Agency
PLC	: Programmable Logic Controller
QCF	: Qassam Cyber Fighters
RAT	: Remote Access Trojan
TCI	: Telecommunication Company of Iran
TIC	: Telecommunication Infrastructure Company
TERENA	: Trans-European Research and Educational . Networking Association

SUMMARY

- Having carried out activities related to cyber defence and internet censorship until 2010, Iran has concentrated on operational cyber capabilities since 2010.
- The National Internet Network project which the Iranian government has begun to build since the 2000s, has been an important step for the isolation in Iran's cyber domain. The national internet policy, which has sparked debates on censorship across the country and the world, has been one of the most prominent practices of Iran regarding its domestic cyberspace.
- Iran's cyber policies and the cyber organizations which it has built within the scope of these policies are being watched with interest in the regional and international arena. The practices adopted by the Iranian government in the cyber domain as a consequence of its exposure to the cyberattacks conducted by the US and Israel, in particular, have been an important milestone for Iran in this field.
- Regarded as the turning point in the building of Iran's cyber capability, the Stuxnet attack has led Iran to lean towards offensive cyber operations.
- As a result of the fact that Iran was perceived as a cyber threat by Israel at the regional stage and by the US in the international arena, the cyber policies of Iran were distinctively shaped in the context of the cyber espionage operations. The advanced cyber actors and the Iranian hacking groups supported by various government agencies have been the main actors of the cyberattacks considered to be of Iranian origin.

Keywords: US, Iran, Israel, Intelligence, Cyber Security, Cyberattack

ÖZET

- 2010 yılına kadar siber savunma ve internetin kontrolü kapsamında faaliyetler yürüten İran, 2010 sonrasında operasyonel siber yeteneklere ağırlık vermiştir.
- 2000'li yıllardan itibaren Tahran yönetiminin inşa etmeye başladığı Ulusal Bilgi Ağı Projesi, İran'ın siber izolasyonunda önemli bir adım olmuştur. İran genelinde ve dünyada sansür tartışmalarına yol açan ulusal internet politikası, İran'ın iç siber uzayı noktasında en belirgin uygulamalardan biri olmuştur.
- Bölgesel ve uluslararası alanda, İran'ın siber politikaları ve bu politikalar bağlamında inşa ettiği siber organizasyonları ilgiyle takip edilmektedir. İran'ın özellikle ABD ve İsrail tarafından siber saldırılara maruz kalması sonucu Tahran yönetiminin başvurduğu siber alandaki uygulamalar, İran'ın bu alandaki önemli kilometre taşı olmuştur.
- İran'ın siber gücünün inşasında dönüm noktası olarak değerlendirilen Stuxnet Operasyonu, İran'ın ofansif siber operasyonlara yönelmesine neden olmuştur.
- İran'ın bölgesel alanda İsrail, uluslararası alanda ise ABD tarafından sıklıkla siber tehdit olarak algılanması sonrası İran'ın siber politikaları, belirgin bir şekilde siber casusluk operasyonları kapsamında şekillenmiştir. Çeşitli devlet kurumlarının desteklediği gelişmiş siber aktörler ve İranlı çeşitli hacker grupları, İran menşeli olduğu düşünülen siber saldırıların temel aktörlerinden olmuştur.

Anahtar Kelimeler: ABD, İran, İsrail, İstihbarat, Siber Güvenlik, Siber Saldırı

چکیده

- ایران تا سال ۱۳۹۸، در حوزه دفاع سایبری و کنترل اینترنت فعالیتهایی داشت. اما پس از آن، توجه خود را بر قابلیتهای عملیات سایبری معطوف کرده است.
- شروع ایران به ساخت «شبکه ملی اطلاعات» از سال ۱۳۸۹، در انزوای سایبری اش نقش مهمی داشته است. سیاست اینترنت ملی که با بروز بحثهایی در ارتباط با سانسور در ایران وجهان مواجه شده، یکی از برجسته ترین برنامه ها در فضای سایبری داخلی ایران بوده است.
- سیاستهای سایبری ایران و سازمانهای سایبری تشکیل شده بر اساس این سیاستها، در عرصه منطقه ای و بین المللی با دقت دنبال می شوند. در نتیجه قرار گرفتن ایران در معرض حملات سایبری، به ویژه توسط ایالات متحده آمریکا و اسرائیل، تهران برنامه های مؤثری را در حوزه فعالیتهای سایبری به اجرا گذارده است.
- عملیات استاکس نت یک نقطه عطفی در ساخت قدرت سایبری ایران به شمار می رود. زیرا باعث شد تا این کشور به عملیات سایبری تهاجمی روی آورد.
- پس از اینکه اسرائیل در سطح منطقه ای و ایالات متحده در سطح جهانی، ایران را به عنوان یک تهدید سایبری مطرح کردند، سیاستهای سایبری ایران به وضوح بر حوزه عملیات جاسوسی سایبری متمرکز شد. در کنار فعالان سایبری حرفه ای که از طرف نهادهای دولتی حمایت می شوند، گروه های هکر ایرانی اصلی ترین بازیگرانی هستند که نامشان در حملات سایبری منتسب به ایران مطرح می شود.

کلیدواژه ها: آمریکا، ایران، اسرائیل، فعالیت اطلاعاتی، امنیت سایبری، حملات سایبری

INTRODUCTION

The concept of power, which is the primary goal of states from a realist point of view, has been intertwined with several elements in time. Having and keeping the influential power, as a result of the developments in military technology and capabilities, is still one of the primary goals for many states. The concept of cyber power, which is a significant factor regarding military power, is one of the crucial elements of power in this context. Through cyber power, states achieve important acquisitions for national security based on both defence and offence.

Iran is one of the states aiming to have regional and international power elements. It has shown remarkable progress on the issues of cybersecurity and operational cyber capabilities after it strengthened its national cyberinfrastructure and information technologies. Due to its regional tensions and its long-lasting conflict with the USA and Israel, it has become necessary for Iran to strengthen its critical national infrastructure, both in civil and public areas.

Iran uses asymmetric capabilities against the organizations that are defined as enemies by Tehran administration in the context of its religious and ideological approaches. It is possible to say that Iran has started to use these asymmetric methods, especially after the economic sanctions. For Iran to struggle against relatively powerful states in the international arena, the asymmetric capabilities that are developed based on cyber technology are sometimes used as a deterrent factor.

Iran's cyber power has been improving as a part of its military power in the last years. 2010, however, represents a turning point for Iran in this context. The Stuxnet attack, which targeted Iran's uranium enrichment centrifuges in Natanz nuclear facilities, directed Iran to increase its investments in cybersecurity. Iran, which has been one of the major operational cyber actors since 2010, currently occupies a significant place among other global cyber actors. It had conducted several defacement attacks through hacktivist groups before 2010. However, after the Stuxnet Attack, it has launched multi-stage attacks through its military, intelligence services, and other forces.

Several states consider Iran's cyber capability as a threat on both regional and international levels. Its offensive cyber capability, based on its strategic institutions like the Islamic Revolutionary Guard Corps (IRGC), Armed Forces of the Islamic Republic of Iran, and Ministry of Intelligence, has made Iran a cyber threat for many states such as the USA, Israel, and Saudi Arabia. It is important to examine strategic elements in Iran which have been improving its offensive cyber capability for the last 10 years.

This research examines Iran's effort to gain operational cyber capability, the state-sponsored cyberattacks, and Iran's multi-stage cyber activities regarding the cyberinfrastructure construction process. The role of Iran's state institutions is also discussed in the analysis, along with the development and characteristics of their role. The study also explores Iran's regional and international cyber-espionage operations, information operations, and disinformation activities on the digital ground.

1. IRAN'S CYBERSPACE

The remarkable development of internet technology since 1974 has created important opportunities and threats for states. Since the global internet network, or cyberspace, in other words, has caused new national security threats and has provided new opportunities for state's interests, it has become a necessity for states to consider the issue with great caution.

Iran is one of the states which evaluates cyberspace as a threat and opportunity. The investments and the policies regarding this issue are significant to show how Iran constructed its cyberspace and its position in this area. It is a known fact that Iran has a significant cyber power because it designates its target as cyberspace in general terms. What is unknown, however, is how Iran succeeded to gain this power.

1.1. Development of Iran's National Internet Infrastructure

Iran is one of the first Middle Eastern countries which connected the internet network in 1993. In the first years, it had internet access only in governmental institutions and in academic network communications. Iran set up its first international internet network through Trans-European Research and Educational Networking Association (TERENA). After a while, it started to serve commercial Internet Service Provider (ISP). In this sense, Neda Rayaneh Communications and Telecommunications Development Institute is a notable institution. Neda Rayaneh, as a nonprofit company, began to serve internet access to all of Iran in February 1995. The company serves as the largest infrastructure server in communication and telecommunication (Open Research Network, 1999, s. 67).

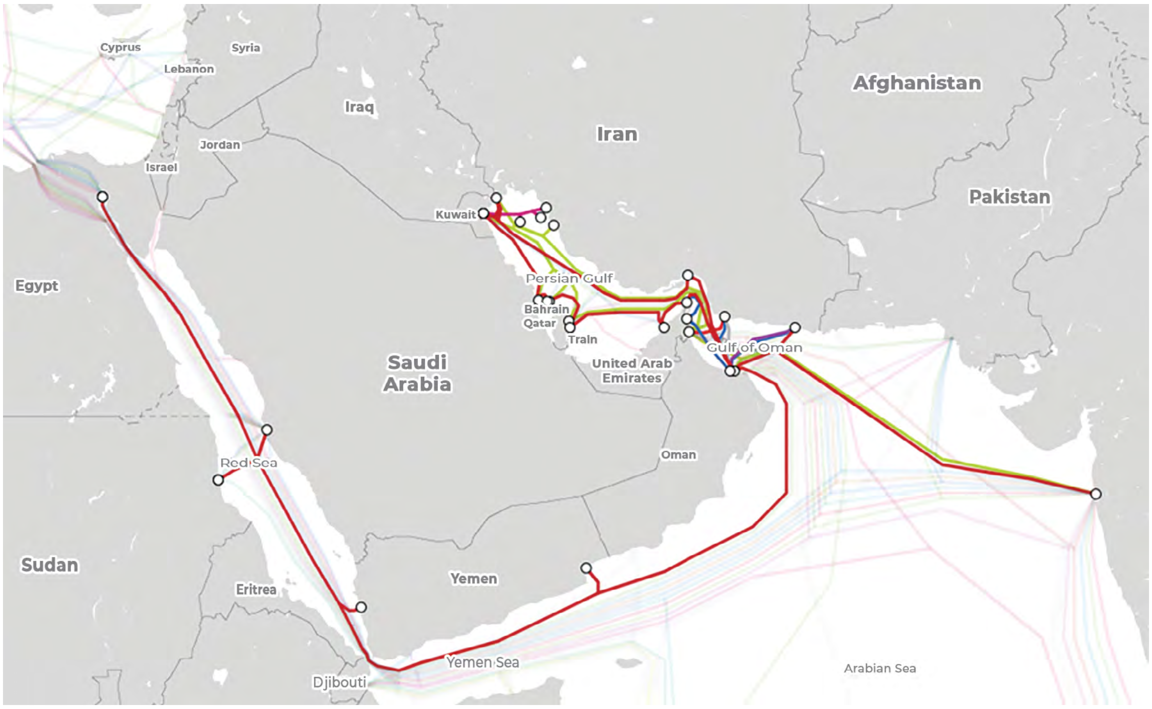
Over 1 million km submarine fibre optic cables that provide the internet and telecommunication servers linked Iran with international networks in the following years. In this context, German Siemens and French Alcatel companies have made crucial investments in Iran, among other countries. It had a significant positive impact on Iran's internet and telecommunication infrastructure.

Siemens is the first foreign company that Iran has got a service for communication and telecommunication infrastructure. The company has been one of the most significant partners for the construction and development of communication infrastructure for many years since 1956. Alcatel is the most significant foreign company that has developed Iran's internet infrastructure (Open Research Network, 1999, s. 94-96). The company established Iran's first submarine fibre optic cable system linked to the United Arab Emirates (UAE). It is currently known as one of the key actors for the development of Iran's internet infrastructure.

The fibre cables, which form the primary infrastructure of Iran's internet network, serve from nine different locations through submarine and land connections. Land connections are provided through Turkey, Azerbaijan, Turkmenistan, and Afghanistan, while the submarine connections are provided through UAE, Kuwait, Iraq, Oman, Qatar, India, and Egypt (Islamic Republic of Iran Ministry of I.C.T., 2010). Submarine connections started with submarine fibre optic links with the UAE in 1992. It has reached the most comprehensive coverage limit with FALCON (FLAG Alcatel-Lucent Optical Network), which was signed in 2006. Lastly, because of the construction of the Oman-Iran submarine connection in 2013, Iran has reached its largest fibre optic network area. According to some news, in 2019, Iran's current national fibre network infrastructure is expected to grow by 20 percent and reach 84,000 kilometers (Tehran Times, 2019).

The foreign companies that make contributions to the development of Iran's internet infrastructure have abstained from cooperation after the economic sanctions against Iran, and several companies quit collaboration. Iran has continued its efforts to improve itself on the issue through

Image 1: Iran's Submarine Cable Networks



Source: Submarinecablemap

the contributions of dozens of local companies. Iran’s arrangement with local companies and a tendency towards a state-sponsored internet infrastructure caused several debates concerning the fact that the infrastructure is constructed and developed to make state interference easy. The main reason behind this debate is the close relationship of the company, which provides internet access, with the Iran government. Indeed, the primary international internet service provider, Telecommunication Infrastructure Company (TIC), is directly controlled by the Ministry of Information and Communications Technology (ICT).

Even though the attempts to interfere with the internet network took place in the 2000s for the first time, more effective and programmed practices have started with the Green Movement protests in 2009. The people had been organizing online platforms like Facebook for the protests that began after the presidential election. However, a while later, they faced internet connection problems. The restrictions to access some internet websites like Google and Facebook and completely blocking some other online platforms paved the way for internet censorship debates in Iran and on the international agenda (ARTICLE19, 2017, s. 11-12).

Many of these platforms were completely blocked after the Green Movement protests and continue to be banned currently. Iran’s persistence in maintaining these bans and desire to control the internet network has resulted in some official initiatives. The most important one is the implementation of the National Information Network.

1.2. National Information Network Project

It is known that Iran tries different paths due to the difficulty of the internet network domination and control. Iran started to develop policies about national internet network after the emergence of internet network and online information services, especially after 2005. It intensified after the Green Movement protests in 2009. Thus an isolated internet network from the foreign one has become one of the primary objectives for Iran.

Iran has planned a secure and effective internet infrastructure in cyberspace since most of its population are active users of the internet and mobile communication. Especially the cybersecurity dimension of the ongoing conflicts with states like the USA and Israel has directed Iran to invest in the national cyberinfrastructure for national security. In this context, Iran prioritizes the development of a local internet network like China and Russia.

The Ministry of Information and Communication Technology authorities made some statements about the construction of the national internet between 2005 and 2006. Nevertheless, they have shared no details about the project (Samii, 2006). The officials declared these initiatives as plans. Any form of written document, plan, or policy towards the content, scope, or the characteristics of the National Information Network project has not come to the agenda. Iran refers to the project as halal and clean internet. It is possible to argue that by this project, Iran aims a secure internet network, which is free from international networks and fully controlled by governmental institutions like China's Great Firewall and Russia's Runet.

The creation of a national internet system has been a point of discussion since 2006 in both locally and internationally. There are controversial assessments about the current stage of the project that has been on the news for almost 15 years.

Official statements of Iran about the national internet also took place in the media between 2010 and 2012. The Ministry of Information and Communication Technology firstly introduced the concept of halal and clean internet in 2010. Following this plan, a unit that included 8000 information technology staff, established in the institution of Basij (IranWire, 2019). In the following years, the national internet has become more and more relatable. It is known that Iran has developed a firewall by its own capability between 2009-2010 and uses it for national internet security.

After the statements of the officials, it was argued that Iran tries to censor the internet and block the encrypted web traffic to possess all internet communication through this project (Ungerleider, 2012). Furthermore, Iran was also accused of developing an internet network under IRGC through the National Information Network project for censorship of the internet (Farivar, 2012).

Iran has taken crucial steps towards cyberinfrastructure until 2012. In this context, Iranian officials declared they started the National Information Network Project and Iran will use a national internet network that is isolated from foreign networks. The National Information Network Project is based on the Fifth Development Plan's decisions about the development of information technologies and consists of three elements: development of an infrastructure of software/hardware, internet content providers, and information services (Islamic Republic of Iran Ministry of I.C.T., 2011).

The main reason for Iran to create an isolated internet network from international networks shows the primary purpose of the project. Iranian officials made several statements concerning the fact that the intelligence services created the international internet network. According to the officials, platforms such as Google and WhatsApp represent a threat for Iranian users because of the espionage activities. Thus, one of the primary reasons for the project is a free and secure internet from foreign networks and threats (ARTICLE19, 2016, s. 18). The National Network Project includes the creation of two different networks for the separation of domestic and international online traffic at the first stage, then reserving and registration of all the websites in Iran in the local servers and ".ir" domain. Then, it will provide domestic email services and searching engines at the third stage (ARTICLE19, 2016, s. 34).

Iran has invested millions of dollars in the project since 2010. The project has almost finalized in 2017 (integration of the governmental institutions, domestic operating system, search engine, messenger, social media, mail server applications) and currently focuses on the research for full isolation. However, according to 2015 data, it is reported that Iran requires additional 3 billion dollars for a full application of the project and for having a developed telecommunication infrastructure (ARTICLE19, 2016, s. 48).

According to the news from May 2019, even though Iran has not made important progress on the national internet infrastructure, it built a security system, the Digital Fortress (Dejfa), for its national cybersecurity (FarsNews Agency, 2019). It has allowed Iran to create a firewall to protect itself from cyber threat actors and the threats of state-sponsored cyber-attacks along with creating a secure internet.

Iran has conducted several types of research on the development of national cybersecurity and internet networks for several years and tried to create state-sponsored domestic solutions to the issues of information technologies. All these efforts of Iran have been interrupted by limited material resources and economic sanctions. In this context, since 2010, the Iran administration has made cooperation with Chinese companies such as Huawei and ZTE on the improvement of information/communication infrastructure rather than focusing on the national internet.

ZTE, as the second-largest telecommunication and information technologies company in China, has been investing in Iran's national information infrastructure for many years. For instance, according to the news in 2012, the Telecommunication Company of Iran (TCI), which dominates Iran's telecommunication and internet infrastructure, has made a 130 million dollars contract with ZTE. According to the contract, Iran bought systems that provide technical surveillance through mobile devices. It is noticeable that many products and software that Iran bought were from US companies (Stecklow, 2012).

It is predicted that Iran continues to cooperate with China on a significant level for its National Information Network Project. In June 2015, the Ministry of Information and Communication Technologies of Iran and Chinese officials agreed to work together on expanding and fulfilling the National Information Network Project (Islamic Republic of Iran Ministry of I.C.T., 2015). Lastly, in 2020, Iran has made a 25 years cooperation agreement with China. As stated in a draft of the agreement, the National Information Network will be implemented with the contributions of Chinese companies (Esfandiari, 2020). Therefore, it is possible to argue that the cooperation between China and Iran about internet and information technologies represents a high-level collaboration and will improve in the next few years.

1.3. The Turning Point of Iran's Cyberspace Policies: The Stuxnet Operation

Cybersecurity, which is seen as one of the main elements of national security policies by states, is a critical issue also for Iran. After land, sea, air, and space, cyberspace has joined as the fifth domain of operation. It is understood in terms of asymmetrical warfare capabilities by Iran. In this regard, it may be said that Iran likes to use cyberspace as a deterrent force for external threats and as a repressive force for the internal ones.

Iran firstly tried to restrict internet access to hinder social media and other digital communication channels to repress the Green Movement protests. It was followed by the ban of social media and several arrests by the Cyber Police. Iran defined mass media and online platforms in terms of significant national security issues during the Green Movement protests. Consequently, it has concentrated on cyberspace policies to establish cybersecurity and to dominate the national internet network (Collin Anderson, 2018, p. 11-12).

Instead of putting cyber defence infrastructure on the agenda to avoid cyber threats during Green Movement protests, Iran chose to apply bans, blocking, and censorship. Even though it started to develop domestic solutions with its cyber defence capabilities against cyber threats, Iran left this policy by 2010. The Stuxnet Operation in June 2010, which caused financial loss along with technological regression in Iran, has become a turning point in this respect. Iran quit its pre-Stuxnet cybersecurity approach and has turned its direction towards offensive cyber capabilities after the attack.

The Stuxnet, which targeted Iran's centrifuges in Natanz nuclear facilities, occupies an important place among specific state-sponsored cyber operations in the international arena. It can be characterized as an operation instead of a cyber attack. Furthermore, since its structure is more complicated than a known virus, worm, trojan, or any other malware and it caused physical harm in the framework of espionage activities, the Stuxnet may be identified as a weapon.

The Stuxnet started to be built in 2005 against specific control units of an industrial control system. After this stage, it started to spread from 2007, and it was detected in 2010, after three years. Its ability to hide for a long time and exploit many vulnerabilities, its complicated structure, and capability to spread and infect the systems without any symptoms represent Stuxnet's quality.

The Stuxnet Operation, which is believed to be developed by US-Israeli cooperation with the contributions of Netherlands and Germany, is a long-term cyber operation that is strategically well thought and well planned. The Stuxnet attracts attention through its quality, its procedure, and its technical content and represents one of the first examples of target-oriented cyber-attacks towards critical infrastructures. It has become one of the crucial subjects in the literature of cybersecurity because it was a destructive cyberattack that is based on the cooperation between states and includes elements of human intelligence (HUMINT) as well.

The process until the detection of Stuxnet may be summarized as follows:

- The intelligence about Iran's establishment of centrifuges in Natanz came forward in 2000.
- The centrifuges that were used in Natanz by Iran were a copy of the stolen designs of a Dutch company, where Abdul Qadeer Khan, known as the nuclear father of Pakistan, used to work. Abdul Qadeer Khan was accused of selling these designs to some states, such as Iran and Libya.

- In 2003, the intelligence services of the USA, UK, and Netherlands infiltrated into the supply network, which consists of the shell companies that help the construction and development of Iran's nuclear program. In this process, the intelligence services of the USA and UK staged a raid on the ship which goes to Libya and carries thousands of nuclear centrifuges elements that are the same models of centrifuges in Natanz's. After the raid, the technical information concerning the centrifuges in Natanz started to be examined. The foundation of the Stuxnet weapon began to build concerning this technical information. In the process, the Stuxnet was updated four times to guarantee the success of the operation.
- At the beginning of 2007, the infiltration to Natanz was planned through a mole who works for the Dutch intelligence service.
- The mole accessed the facility in the role of a technician in a shell company that was established by the USA and Israel.
- The mole has accessed Natanz in the spring of 2007. Even though he could not get involved in the configuration of centrifuges directly, he was able to collect information about the devices and their configurations. He got the necessary information for the success of the virus by visiting the site several times. Later, he brought the virus physically in a USB drive to the facility and uploaded it to the systems (Kim Zetter, 2019).
- The Stuxnet had worked for three years without detection until it was detected in June 2010.

If Stuxnet was not detected, it would cause bigger damage to the Iran nuclear program and its accumulation. The main reason for the failure of the operation may be seen here because the actors who created Stuxnet added several numbers of expanding mechanisms. It caused Stuxnet to be detected also in other countries and resulted in the destruction of Stuxnet. As a result, after the exposure of the operation, Iran executed two people who worked in Natanz and who were thought to have an operational role. The fate of the Dutch mole is still unknown.

The process of the detection of Stuxnet is also important and complicated, at least as much as its construction process and intelligence collection process. Belarusian cybersecurity researchers, with whom Iran was in strong cooperation, became one of the key actors of Stuxnet's detection. The most significant actor among them is Sergey Ulasen, who currently works in Kaspersky.

The Stuxnet, which was revealed by Belarusian cybersecurity researcher Sergey Ulasen, was detected firstly in the systems of some state institutions and private companies. It was thought to be a basic virus at the first stage, but after months of research, this extraordinary weapon appeared to be developed for different purposes. The technical analysis showed that the Stuxnet was looking for "0day" flaws (software and hardware weakness which nobody is aware of, including its manufacturer until its detection) in the systems it infected. It was primarily trying to reach an address in the Siemens Step7 PLC (Programmable Logic Controller) which was used in Iran's Natanz nuclear facility. To do so, Stuxnet was looking for vulnerabilities in the Windows operating system, a flaw in Siemens PLC systems, and weakness in the centrifuges' frequency inverter drivers (Nicolas Falliere, 2010).

The Stuxnet, which used several different hardware and software ways to reach the PLC system, also took advantage of human intelligence against any case of failure. The most critical milestone of the operation was when the Dutch spy, also known as the mole, who worked in Natanz nuclear facility, attempted to infect Stuxnet through a USB drive.

Image 2: The Stuxnet as a Joint US-Israeli Effort That Targets Iran

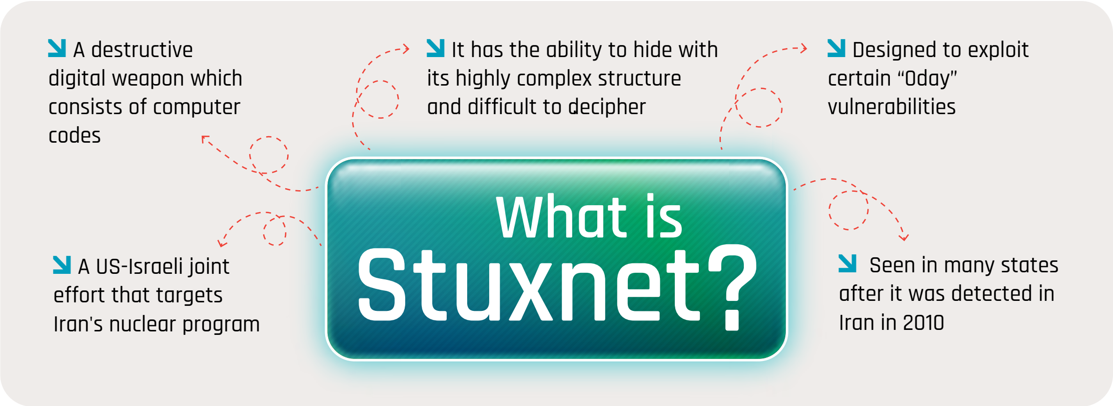
Source: Yahoo News

After it reached its targeted system, Stuxnet caused to overheat almost a thousand uranium enrichment centrifuges and consequently their destruction. This sophisticated operation, which is predicted to hinder the progress of Iran's nuclear program for two years, represents the significance of the Stuxnet concerning its damage to Iran's national cybersecurity.

Iran has increased its retaliatory cyberattacks against the USA and Israel, while it tried to compensate for the losses in Natanz after it inactivated Stuxnet with the help of companies such as Kaspersky and Symantec, in addition to Ulasen. Iran has changed its cyberspace security policies after Stuxnet significantly damaged its national cyberinfrastructure along with its harm to the Natanz nuclear facility. Nevertheless, it should be noted that Iran has also a tendency towards military aggression like Russia. Thus, Iran has given weight to offensive strategies for its national cybersecurity instead of defensive strategies. It may be seen through state-sponsored cyber operations and global cyber operations that are exercised by special units of the state. Iran interpreted Stuxnet Operation as a part of cyber warfare, and it has specified offensive policies including cyber sabotage and cyber espionage activities against some states that are «the enemies» like the USA and Israel. Iran has been trying to strengthen and improve its technology, its number of relevant personnel, and its infrastructure, especially through IRGC and has started to act strategically in cyber warfare (Spadoni, 2019).

The emergence of Duqu and Flame viruses after Stuxnet, which also aimed at Iran's nuclear program and damaged functions of some public institutions, speeded up the determination process of these policies. Even though Flame, which was active in 2010 and identified as SkyWiper in 2012, is like Stuxnet, it is characterized as a much more complicated and powerful cyber weapon. It differs from Stuxnet by

Image 3: What is Stuxnet?



What is Stuxnet?

A destructive digital weapon which consists of computer codes

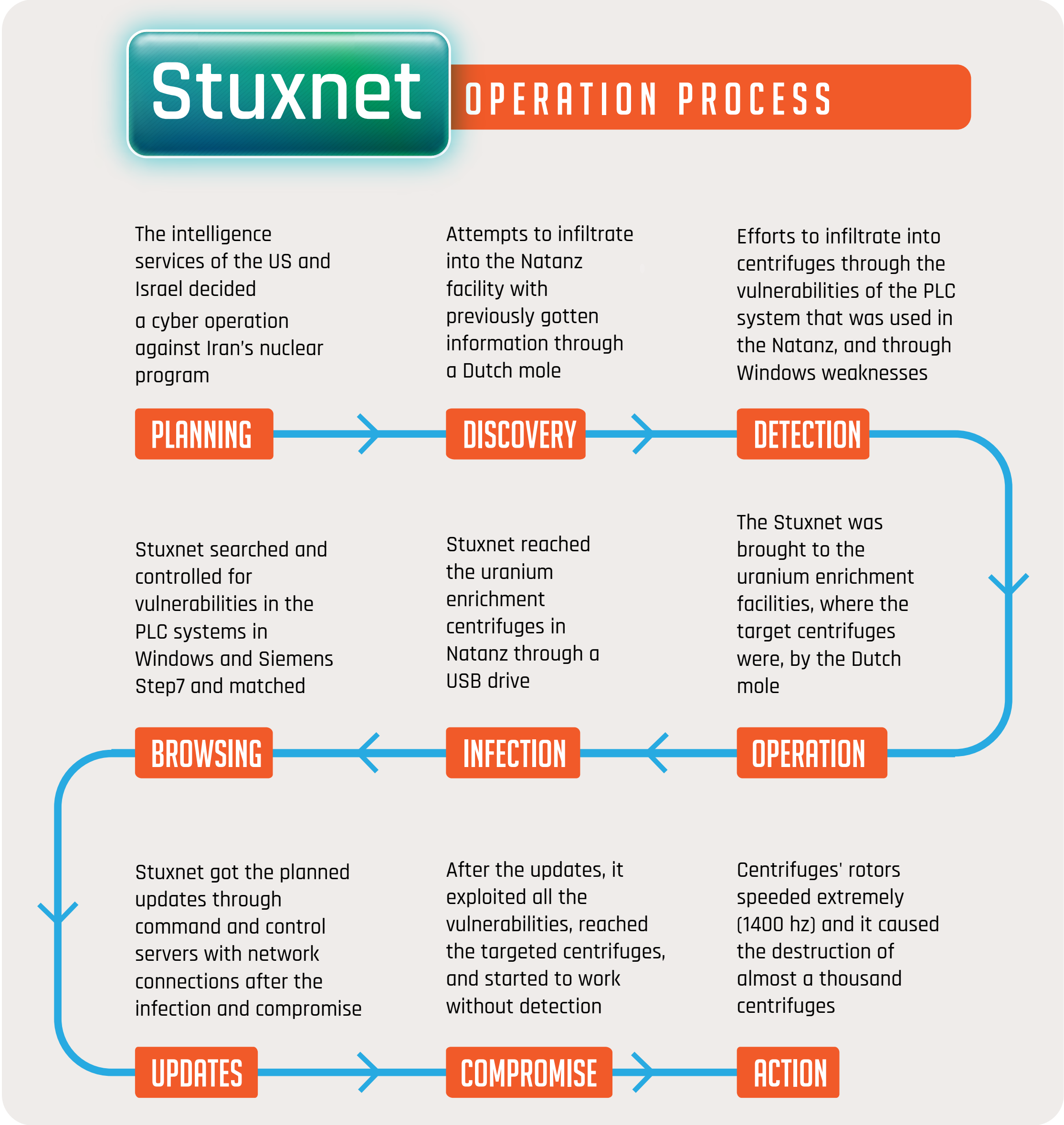
It has the ability to hide with its highly complex structure and difficult to decipher

Designed to exploit certain "0day" vulnerabilities

A US-Israeli joint effort that targets Iran's nuclear program

Seen in many states after it was detected in Iran in 2010

Image 4: The Process of the Stuxnet Operation



Stuxnet OPERATION PROCESS

PLANNING: The intelligence services of the US and Israel decided a cyber operation against Iran's nuclear program

DISCOVERY: Attempts to infiltrate into the Natanz facility with previously gotten information through a Dutch mole

DETECTION: Efforts to infiltrate into centrifuges through the vulnerabilities of the PLC system that was used in the Natanz, and through Windows weaknesses

OPERATION: The Stuxnet was brought to the uranium enrichment facilities, where the target centrifuges were, by the Dutch mole

INFECTION: Stuxnet reached the uranium enrichment centrifuges in Natanz through a USB drive

BROWSING: Stuxnet searched and controlled for vulnerabilities in the PLC systems in Windows and Siemens Step7 and matched

UPDATES: Stuxnet got the planned updates through command and control servers with network connections after the infection and compromise

COMPROMISE: After the updates, it exploited all the vulnerabilities, reached the targeted centrifuges, and started to work without detection

ACTION: Centrifuges' rotors speeded extremely (1400 hz) and it caused the destruction of almost a thousand centrifuges its purpose to steal information from the target instead of damaging it. The source of the weapon that was first detected in Iran is still unclear. Nevertheless, allegedly it was used in an operation in the context of US-Israel cooperation like it was in the Stuxnet (sKyWIper Analysis Team, 2012).

Duqu, which emerged in 2011 and included similar codes with the software of Stuxnet and Flame, revealed to be developed by the threat actors who created Stuxnet or who have access to the source code of Stuxnet. The purpose of Duqu is known as getting data from the target system and gathering intelligence data and sensitive information for future attacks from the institutions like industrial infrastructure and system manufacturer (Symantec, 2011).

The Stuxnet operation and other cyberattacks against Iran became a milestone for the government. These operations caused physical damages and revealed the vulnerabilities of Iran's critical facilities along with the weaknesses of its national internet infrastructure. After this revelation, Iran has taken steps towards cyber defence policies. After it comprehended the limitation of its cyber capability, Iran started to give weight to offensive cyber capabilities.

By its defensive and offensive cyberspace activities, Iran aims to avoid any kind of future damages or losses as a result of potential threats. These activities started with the instruction of the Supreme Leader Khamenei and exercised by Iran intelligence services and other security agencies.

2. IRAN'S CYBER INSTITUTIONS AND ORGANIZATIONS

Iran, like many other states, has several institutions and organizations that engage in cyber defence and cyberattacks. Some of these institutions and organizations are directly affiliated with the government. Some others are, on the other hand, indirectly supervised by the government. Furthermore, there are also organized cyber threat actors that are not affiliated with the government but cooperate with certain institutions when it is required.

Iran's ability for retaliation has been a point of discussion, especially after the USA's and Israel's cyber espionage and cyber operations against Iran. After 2010, a high-level initiative within the state has taken political steps toward developing Iran's offensive and defensive capability.

In this context, several institutions concerning cyber defence and cyberattack have been established in different units. There are also state-sponsored organizations that are established with the same purpose. Iran's institutions that play a role in its cyberspace may be categorized into two groups: state institutions and state-sponsored institutions.

2.1. Effective State Institutions in the Cyber Activities

The state institutions, which play a role in Iran's cyberspace, carry out both offensive and defensive activities. As noted above, the state institutions are fully responsible for national cyber activities in Iran. The Iran government coordinates and controls cyber defence as well as operational capabilities and abilities for cyberattacks.

In this regard, the Tehran administration has an important role in national and international cyber activities that are exercised by the state institutions. Generally, Iran's cybersecurity policies and strategies are determined by a council that is led by the Supreme Leader Khamenei. The intelligence services and other security agencies implement operational and military dimensions of cybersecurity.

As well known, there is no detailed information about the state organizations which are effective in Iran's national and international operational cyber activities. Therefore, it is possible to mention these state organizations, state-sponsored organizations, and their activities shortly thanks to the information that is gathered from open sources (some intelligence services and security agencies' reports, the news, analysis of professional companies that have expertise on the issue).

a) The Supreme Council of CyberSpace: The Supreme Council of CyberSpace, which was established with the instruction of Khamenei in 2012, is responsible for coordination and policy-making for national cybersecurity and information security under the supervision of the president. The Council includes the President, the Speaker of Parliament, head of the Islamic Republic of Iran Broadcasting, the Commander of the Armed Forces, the Commander of the IRGC, the Minister of Defence, the Minister of Information and Communication Technologie, the Chief of Police and some former top-level officials and academics. The primary responsibilities of the Council may be summarized as follows: protecting the people, the state, and the cyberspace from any internal or external cyber threats, making cooperation with the business partners, the academy, and others regarding cybersecurity, preparing the law, regulations, and instructions about national cybersecurity (SmallMedia, 2017). After the establishment of the Council, all the works and policies regarding Iran's public and private internet and information infrastructure have been coordinated under the National Cyber Space Center. It is also known that the Council determined the policies, which paved the way for internet censorship debates, and plans towards national internet network (Islamic Parliament Research Center of The Islamic Republic of Iran, 2012). It may be argued that Iran's cybersecurity strategies are specified in the Council.

b) National Passive Defense Organization: The National Passive Defense Organization, which works as a special unit under the Armed Forces of the Islamic Republic, aims to protect Iran's national critical infrastructure from cyberattacks (Bastani, 2012). It is the Organization's responsibility to identify external threats for Iran's cyberspace, discourage potential threats, and prevent them.

c) The Cyber Defense Command: The Cyber Defense Command was established under the National Passive Defense Organization in November 2010. It is known as the primary institution that is responsible for Iran's national cyber defence. The organization comes into prominence with its defensive cyber activities. It was created thanks to the offer of the National Passive Defense Organization after the Stuxnet Operation caused critical damages to the nuclear program in November 2010 (Bastani, 2012). Even though The Cyber Defense Command is claimed to carry out cyber defence activities only, several experts indicate that the Command also has the capacity for offensive cyber activities.

d) IRGC Electronic Warfare and Cyber Defence Organization: IRGC Electronic Warfare and Cyber Defence Organization are associated with IRGC. According to official statements of the USA, the organization is under the control of IRGC or acts in the name of it (U.S. Department of the Treasury, 2018). The primary purpose of the organization is claimed to be involved in the operational activities in the context of electronic warfare. Despite the fact that there is no detailed information about the organization, the cybersecurity companies in Iran, like Net Peygard Samavat Company, are known to provide technical support and consultation to the organization.

e) Basij Cyber Organization: The Basij, which works directly under the roof of IRGC, has a special cyber structure. The Basij Cyber Organization, also known as the Basij Cyber Council, which is predicted to be reached full operational capacity in 2009, differs from other organizations with its focus on internet operations. It includes units that are involved in activities in the areas of education, digital content, and social media. Most of the members of the organization are predicted to be not experts. Their practices comprise basic cyber activities, including information operations through blogs and attacks on websites. Apart from these, some hackers, who are controlled by IRGC, are also claimed to used by the organization (IranWire, 2019).

f) The Ministry of Intelligence and Security (MOIS): Ministry of Intelligence and Security, which is the official intelligence organization of Iran, is responsible for foreign intelligence operations, disinformation, and propaganda. It is similar to IRGC in the context of intelligence and security. Thus, the acts of the two institutions usually overlap, especially on technical issues. In the cyber area, on the other hand, the Ministry of Intelligence and Security is known to target some opposition politicians and journalists and to use technical surveillance technologies in its intelligence operations, unlike IRGC. The ministry is claimed to use some shell companies like Rana and Mabna institutions in its active cyber operations and intelligence activities. Moreover, the University of Isfahan and the University of Tehran are known to provide technical support to the ministry. The main difference of the Ministry from the other institutions is its use of Advanced Persistent Threat (APT) groups in official cyber activities (Recorded Future - Insikt Group, 2020). Some APT groups such as APT34, APT39, and Magic Kitten are reported to be linked directly to the ministry. The institutes, the universities, and the APT groups that are mentioned will be discussed in the third chapter.

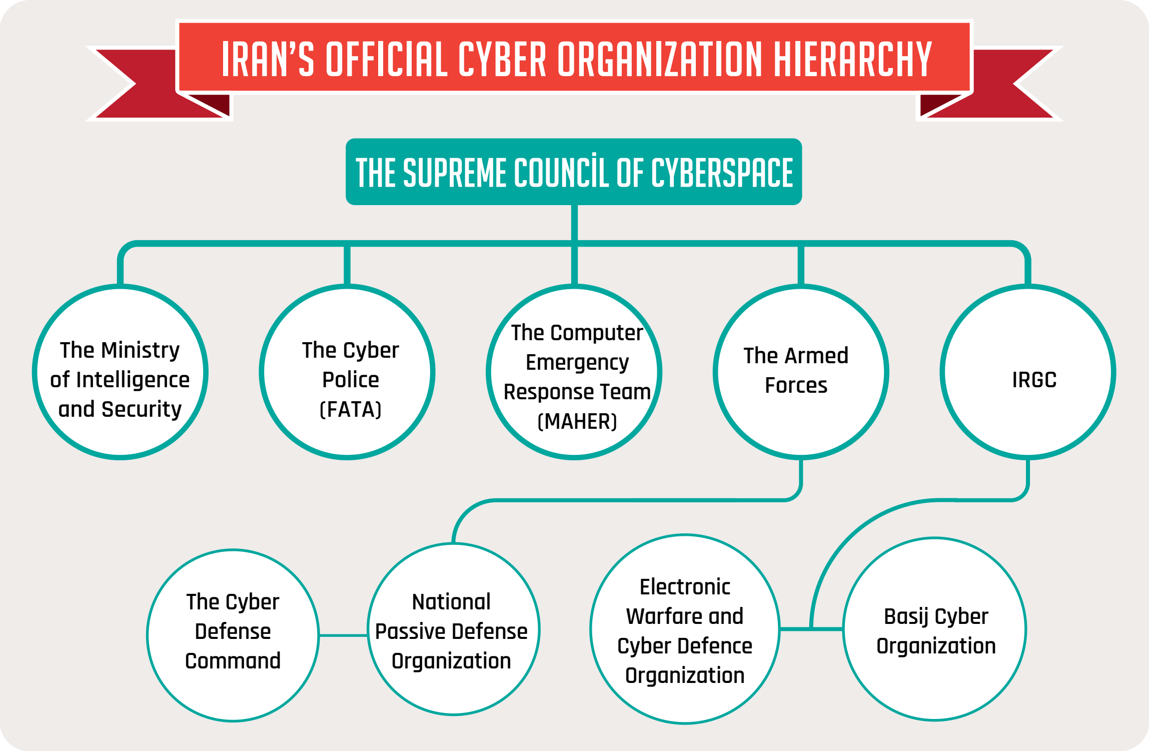
g) The Cyber Police (FATA): The cyber police unit FATA was established in 2011, after the Green Movement protests of 2009, to fight against the crimes on the digital ground. Cyber police, which aims to eliminate cyber crimes in general terms, fights against identity/data theft, online information operations, and cyberbullying in cyberspace. FATA is believed to play a significant role in controlling and monitoring Iran's so-called halal internet, National Information Network. The organization is also claimed to be active in the internet restrictions and the operations against anti-government protestors on online platforms (especially in social media). (Small Media, 2019).

h) Computer Emergency Response Team (MAHER): MAHER is established for improving Iran's capability to respond to cyber issues. Like other states' Computer Emergency Response Teams, it consists of information security specialists. MAHER has several responsibilities, including monitoring and analyzing national cyber cases for 7/24, responding to attacks or operations, collaboration with state institutions or the private sector, and organizing training and drills.

2.2. State-Sponsored Cyber Organizations

Operational defensive cyber activities in Iran are managed and controlled almost completely by state institutions. Offensive cyber activities, on the other hand, include the contributions of universities, institutes, private companies, and advanced hacker groups along with state institutions.

Image 5: Iran's Official Cyber Organization Hierarchy


IRAN'S OFFICIAL CYBER ORGANIZATION HIERARCHY
THE SUPREME COUNCİL OF CYBERSPACE
The Ministry of Intelligence and Security
The Cyber Police (FATA)
The Computer Emergency Response Team (MAHER)
The Armed Forces
IRGC
The Cyber Defense Command
National Passive Defense Organization
Electronic Warfare and Cyber Defence Organization
Basij Cyber Organization

Iran's offensive cyber operations before the 2010 Stuxnet Operation requires a closer look. Through underground hacker groups, Iran had several cyber operations against its political or ideological enemies, especially against Western states, in the context of its national interests. Despite the fact that the state-sponsored cyber groups had launched basic cyber operations before 2010, in the following years, they have reached the capability for advanced cyber attacks against specific targets in the scope of intelligence operations with the help of APT groups. The relevant cyber organizations are as follows:

a) Iran Hackers Sabotage (IHS): The hacker group, who calls themselves Iran Hackers Sabotage and has been active since 2004, draws attention with their attacks towards several websites. The group, which specifically targeted the USA, UK, France, Israel, and Saudi Arabia, has engaged in website defacement, which includes changing and defacement of the contents of the websites. They also sent several political and ideological messages (Denning, 2017).

b) The Ashiyane Security Group: The hacker group, also known as the Ashiyane Digital Security Team, represents the basis of current hacker groups in Iran. Like IHS, the Ashiyane hacker group has actively engaged in website defacement since 2006. The group that is still active is believed to be the basis of prominent APT groups in Iran and controlled directly by IRGC. As the founder of the Ashiyane group, which is the principal actor in the attacks against conflicted states, Behruz Kamalian is the person who carried out the operations to Israel's official websites between 2006-2008. Even though he stated Ashiyane groups continue their activities independently like an independent company, it is known that the group cooperates with Iranian intelligence services and military institutions (Spadoni, 2019).

The closure of all cybersecurity forums except from the Ashiyane group in 2009 shows the close relationship between Kamalian's team and the Iran government. According to some technical indications, the group has approximately 20,000 forum members. After the split of the group in 2018, the operational team headed towards several areas. Kamalian, known as the father of hack operations in Iran, provided technical support for offensive cyber tools to the Iran government after the 2010 Stuxnet Operation. Kamalian is predicted to continue to serve in Ashiyane Digital Security Team with a few people (Recorded Future - Insikt Group, 2019).

c) Cutting Sword of Justice (CSJ): Even though there is no detailed information concerning the CSJ, it drew attention to its Shamoon Operation against Aramco Oil Company in Saudi Arabia in 2012. The group is believed to be controlled by the Iran intelligence services. On their websites, CSJ declared that they are behind the Shamoon Operation, which erased tens of thousands of data from Aramco through a website and known as wiper malware. The Shamoon Operation, which attracted attention in the rest of the world more than Saudi Arabia, is known as the only operation this group had done. Furthermore, this operation represents Iran's first professional cyber espionage activity and the cyberattack that caused damage.

d) Qassam Cyber Fighters (QCF): QCF is a state-sponsored hacker group in Iran that aims to sabotage and carry out destructive cyber attacks. The organization did several attacks against the USA between 2012 and 2013. Iran has concentrated on the offensive cyberattacks after the Stuxnet, and these attacks are aimed particularly at the USA. QCF took responsibility for Operation Ababil, which targeted the biggest financial institutions in the USA. The attacks of the organization were mostly based on Distributed Denial of Service (DDoS). QCF has provided significant capabilities to Iran like CSJ (Recorded Future - CHRIS, 2013).

e) Ajax Security Team (Flying Kitten): This hacker group, currently known as Flying Kitten[1] was active between 2010 and 2014. It frequently used the spear-phishing attack as an attack method in its cyberespionage operations. The Ajax Security Team is known as Flying Kitten since 2014. Iran launched its first specific cyber-espionage operations through Flying Kitten (Fire Eye, 2014).

f) The Mabna, Rana, and Nasr Institutes: The Mabna Institute, also known as TA407, Cobalt Dickens, and Silent Librarian, is one of the most influential civil organizations on cyber domain in Iran. The company was established in 2013 allegedly to launch cyber operations to foreign academic sources of other states. The members of the institute are known to work in collaboration with IRGC and other critical organizations, which occupy an important place in Iran's defence and security. Furthermore, the institute is believed to provide technical support for the cyber operations of APT34 and APT39. According to the FBI, Mabna Institute is one of the major companies which provide funds to hacker groups and coordinate hacker operations that target more than 100,000 academics from different universities of 21 countries (FBI, 2018). Especially hacking operations that aim to gather intelligence for the IRGC are successful to acquire academic documents and critical data from the top universities worldwide. The institute has also targeted 50 worldwide private companies (mostly from the USA) (Tabansky, 2018).

A similar organization, Rana Institute, conducts activities that aim at disinformation. In contrast to Mabna, it is associated with the Ministry of Intelligence rather

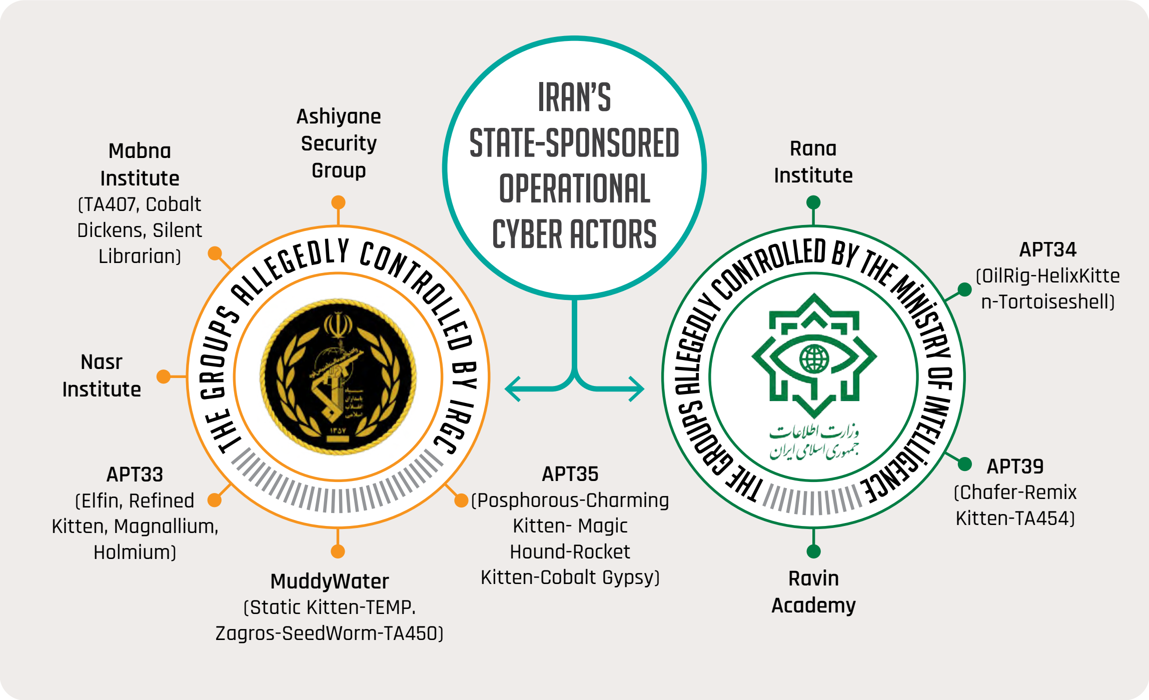
[1] Iranian APT groups are usually defined as "Kitten". These sorts of code names are used by states and cyber security companies for the countries such as Russia, China, and Iran. Russia is known as Bear, China as Panda, and Iran as Kitten.

than IRGC. Furthermore, members of the Rana are also known to have a relationship with the APT39 group, like Mabna. According to the leaked information, Rana Institute is divided into two branches. The first branch, which is responsible for the development of malware and tools, focuses on cyber espionage activities. The second branch, on the other hand, involves cyber attacks, that is known as social engineering, and cyberattacks that use spear-phishing method for identity chasing. It is also known that some members of the institute work at the University of Tehran and Sharif University of Technology and provide technical support from these universities. One of the primary sources of the leaked information concerning the Rana Institute is Masoud Molavi Vardanjani, who is also known in Turkey. Molavi was killed in Istanbul on November 14, 2019, by the Iran intelligence service after he leaked information about Rana Institute and Iran's operational cyber actors through its Telegram channel Black Box (Clearsky Cyber Security, 2019).

Lastly, there is little information about the Nasr Institute since it is not active as much as Mabna and Rana. In its active years between 2011 and 2013, Nasr Institute helped especially APT33 group in the cyber operations which use backdoors and Remote Access Trojan (RAT). Several reports of the specialists also state that the Institute is associated with QCF's DDoS attacks, Operation Ababil, that aimed at financial institutions of the USA (FireEye, 2017).

g) The APT Groups and The Other Actors: Iran's most active and most sophisticated organized groups, that carry out cyber operations, are the APTs since 2011. These groups are called by the code names which are given by the USA or by the prominent international cybersecurity companies. They conduct a wide range of operations, including cyber espionage, financial operations, critical infrastructure attacks, and data leakage. The most known APT groups are APT33 (Elfin, Refined

Image 6: Iran's State-Sponsored Operational Cyber Actors


IRAN'S STATE-SPONSORED OPERATIONAL CYBER ACTORS
THE GROUPS ALLEGEDLY CONTROLLED BY IRGC
Mabna Institute (TA407, Cobalt Dickens, Silent Librarian)
Ashiyane Security Group
Nasr Institute
APT33 (Elfin, Refined Kitten, Magnallium, Holmium)
MuddyWater (Static Kitten-TEMP. Zagros-SeedWorm-TA450)
APT35 (Posphorous-Charming Kitten- Magic Hound-Rocket Kitten-Cobalt Gypsy)
THE GROUPS ALLEGEDLY CONTROLLED BY THE MINISTRY OF INTELLIGENCE
وزارت اطلاعات
جمهوری اسلامی ایران
Rana Institute
APT34 (OilRig-HelixKitte n-Tortoiseshell)
APT39 (Chafer-Remix Kitten-TA454)
Ravin Academy

Kitten, Magnallium, Holmium), APT34 (OilRig, Helix Kitten, Tortoiseshell), APT35 (Phosphorus, Charming Kitten, Magic Hound Ajax Security, Rocket Kitten, Saffron Rose, Cobalt Gypsy), APT39 (Chafer), CopyKittens and MuddyWater (TEMP.Zagros, Seedworm).

All of the APT groups that are originally from Iran are state-sponsored, like Russia and China. In other words, these groups are sponsored and controlled by the Ministry of Intelligence, IRGC, and the state's other security institutions. The most active ones among the groups are APT33, APT34, and APT35. They usually carry out operations against governmental institutions, critical infrastructures, energy, telecommunication, and finance sectors, universities, think tanks, and top-level bureaucrats of the USA, Israel, UAE, and Turkey. The APT groups, which occupy a significant place in Iran's operational cyber capabilities, are usually used in strategic intelligence activities.

The activities and targeted state institutions of these APTs will be examined in the third chapter, along with non-state actors and companies. Apart from APT groups, there are some hacker groups or hacktivist groups which have been active lately. The cyber operations of these cyber threat actors such as BlackShadow and Pay2Key will also be explored in the third chapter.

3. IRAN'S CYBER OPERATION

Iran carries out both domestic and foreign cyber operations through its offensive cyber capacity that it has gotten since 2010. The activities of the law enforcements in Iran, which plays an important role in the practice of cybersecurity policies, deserve attention. The intensification of the surveillance policies against dissidents in Iran has caused negative reactions and concerns both in the region and the international arena.

The activities of technical intelligence, which is one of the technology-based practices, are another dimension of the Tehran administration's operations. The dissident journalists and activists in Iran are tracked and monitored through mobile devices, surveillance cameras, and smart technologies. With the development of the national internet network, the intelligence activities against Iran citizens, through censorship policies and monitoring network traffic, have been also a point of discussion (REF World, 2015). These activities are operated largely by Iran's cyber police FATA.

It is claimed that the APT organization, along with the law enforcements, also targets the individuals in Iran. These "internal targets" include the opponents and certain ethnic groups. The APTs in Iran, as FATA doing, can work to gather information about these groups and to control them through surveillance, monitoring, and chasing.

The other security organizations such as the Ministry of Intelligence and IRGC also use these kinds of surveillance methods to arrest the members of the dissident groups. The APT groups come into prominence in these activities. For instance, according to an FBI report, the Rana Institute, allegedly a shell company of APT39 that is directly linked to the Ministry of Intelligence, carries out operations of repression and intimidation against opponent groups (FBI, 2020).

These activities of the APT groups, which are claimed to have close relations with the Iran government, confirm the allegations. Furthermore, there are some other cyber attacks of other actors. For example, some cyber actors, who define themselves as Iran's patriot hackers, hacked the websites of the opponent groups by the website defacement method and shared pro-Iran messages.

Iran's domestic cyber practices include some application-based activities, along with eavesdropping mobile devices and monitoring through some technical intelligence tools. As well known, Iran, like China, bans Western-based technologies and platforms in the country. Especially US-based platforms Google, Facebook, and their applications such as YouTube and WhatsApp along with social media platforms like Twitter are occasionally banned or limited for access.

The Iranians who want to use these applications get access to the platforms through VPN services. In addition to banning these websites, the Iran administration also encourages the use of the domestic versions of these platforms. The National Cyberspace Centre, which is established by Iran's Supreme Council of Cyberspace, supports the usage of the applications such as Soroush, iGap, BisPhone Plus, and Wispi, which are developed by Iranian specialists.

Iran has also encouraged the usage of Telegram and Hotgram that are developed through Telegram's open-source software. Nevertheless, Google and Apple removed these applications because of the complaints of Iranian users concerning the fact that the applications are used for espionage activities by the Iran government (Tehran Times, 2019). The security/privacy-oriented Signal application, which has become highly popular after the WhatsApp scandals, is also banned in Iran. As seen, the Iran administration uses several tools and methods to control mobile communication and the internet in the country.

The domestic cyber operations of the Iranian government are examined above. Now, Iran's foreign cyber operations, which is the main issue of the paper, will be examined below through the APT groups and the cyber threat actors' global cyberattacks and the information operations. Iran's policies towards its national interests place Iran in an offensive position in cyberspace. In this regard, it should be noted that some part of the Iran-originated cyber operations is only allegations. However, these allegations have a high degree of accuracy.

3.1. Allegedly Iran-Originated Offensive Cyber Operations

Most of the Iran-originated cyber operations targeted the USA, Israel, and Saudi Arabia. It is also important to state that the relevant cyber operations were revealed by US and Israeli companies. The security units of the USA and Israel are able to detect the Iran-originated cyber-attacks through their cyber defence systems (like firewalls, traps, traffic monitoring, system analysis). Furthermore, these attacks are also mentioned in the reports of international cybersecurity companies that are not US or Israel originated, such as Kaspersky, ESET, and Sophos.

As is mentioned in the second chapter, the principal actors in Iran's regional and global cyber operations are the APT groups. The regional and global activities of these APT groups, along with other hacker groups, represent Iran's operational cyber capacity. In this context, Iran's cyber operations against critical state institutions and private companies of almost 40 countries, primarily the US and Israel, are worth attention. These operations may be listed through their cyber actors as follows:

a) The Mabna, Rana, and Nasr Institutes: The names of the nine members of the Mabna Institute, which was heard for the first time after the USA revealed a cyber-espionage attack in

2018, are on the FBI most wanted fugitives list. These members, whose names and photos are included in the FBI reports, have been accused of a state-sponsored cyber-espionage operation against the USA. They are known to work for the IRGC and to have close relationship with the Iranian government. The nine members are claimed to carried out cyber operations against some of the US universities, private companies, and some of US state institutions (FBI, 2018).

As noted in the second chapter, the Mabna Institute has been active since 2013. When cyber actors such as Silent Librarian APT, Cobalt Dickens and TA407 were realized to be overlapped, it was named the Mabna Institute. As stated in an FBI report, the cyber actor, known as the Silent Librarian APT in 2017, had 127 different domains that used the spear-phishing method. It is found that there are over 750 cyber-attacks that are associated with Silent Librarian until September 2013. The attacks targeted more than 300 universities in 22 different states. According to the FBI report, engineering and medicine disciplines were exclusively targeted (Hassold, 2018). Reports show that these types of cyberattacks have been intensified since 2019 and continue by aiming at several universities and academics, especially in the USA and Europe (RISKIQ, 2020).

As another institute, Rana Institute carries out cyber operations through similar methods. It has been known since 2019 thanks to the information that Vardanjani leaked, who was assassinated in Turkey as examined in the second chapter. The institute is stated to aim at all the Iranians who live in the country or abroad (Clearsky Cyber Security, 2019). On September 17, 2020, the United States Department of State declared that the Rana Institute, which involves active cyber operations in the name of Iran, and 45 people from APT39, that is linked to the institute, have been added to the sanction list. It is reported that Iran has used offensive cyber attack tools for targeting and monitoring Iranian opponents, journalists, former government officials, environmentalists, refugees, university students, academics, and international non-governmental organization employees through the Rana Institute for the Ministry of Intelligence (U.S. Department of State, 2020).

The 45 people that were added to the sanction list by the US Department of the Treasury are reported by the FBI to be managers, programmers, and advanced hackers in the Rana Institute. These people specifically focused on the targets, which are defined as threats by Iran's Ministry of Intelligence, and provided support for the cyber-attacks of the Ministry on several occasions. The FBI has attributed some operations directly to the Iran Ministry of Intelligence through some technical indicators (IOC -Indicator of Compromise) for the first time (FBI, 2020). According to several reports, even though the Rana Institute uses different TTP (Tactics, Techniques, and Procedures), its primary method is spear-phishing to get the targets' data by data theft.

Lastly, the Nasr Institute is less active than the other two institutes. As stated in the second chapter, the Nasr Institute is usually associated with the APT33 group and conducts cyber-espionage activities along with targeting the universities like the other institutes. According to a report in 2017, a backdoor that the APT33 used is linked to a member of the Nasr Institute. Furthermore, it is noted that Iran uses the Nasr Institute as well as other shell companies to cover the actors of state-sponsored offensive cyber operations. Thus, several specialists argue that the Nasr Institute is associated with the APT33, APT35, and MuddyWater and conducts joint actions like Ababil Operation in 2013 (Recorded Future - Insikt Group, 2019).

b) APT33 (Elfin, Refined Kitten, Magnallium, Holmium): APT33, which has been active since 2013, is one of the most effective APT groups in Iran. The group, which has directly linked to IRGC, targets specifically the USA, Israel, and UAE and involves in cyber espionage operations against the state institutions and aviation, industry, and energy sectors. It has conducted many cyber operations against more than 50 institutions and organizations in the relevant states (Symantec, 2019).

The APT33 group, which has had several names over time, has specialized in hacking the target's internet infrastructure and establishing a command and control (C&C) system. There are tens of factual reports concerning the APT33, which has a wide scope of targets. The group operates against the sectors of chemistry, engineering, finance, aviation, technology, telecommunication as well as state institutions. It has become popular with its cyber-espionage attacks and held responsible for the Shamoon Operation, which targeted Saudi Arabia's Aramco Oil Company in 2012 and caused serious damage (FireEye, 2017). Because the CSJ group also played a role in the Shamoon Operation, as stated above, it is possible to argue that the CSJ group is integrated with the APT33. The group has a major operational capacity besides its potential for the attacks that causes physical damage on the infrastructures of official/critical institutions and currently continues its activities. The targets of the group includes also the defence industry institutions in Turkey.

Image 7: APT33[2]

Source: FireEye

c) APT34 (OilRig, Helix Kitten, Tortoiseshell): The APT34 group, which is associated with the Iran Ministry of Intelligence and active since 2014, has targeted several state institutions in Turkey and the Middle East. The group mostly carries out cyber-espionage operations and leaks into the targets through malicious email attachments to gather intelligence data. Some reports, where the group is mentioned as OilRig, state that APT34 may have destructive cyber capacity like APT33. These reports also indicate that APT34 regularly attacks Saudi Arabia's Aramco Oil Company with the updated versions of the Shamoon virus. Except for APT33, APT34 is also known to operate against energy and oil companies of Saudi Arabia through wiper attacks on the data of targeted infrastructure by the updated Shamoon viruses. The APT34 continues its operations as the most active cyber threat actor in Iran. The identities of more than 20 Iranian, allegedly the members of the group, are revealed on the Telegram.

Another point that is worth mentioning about the APT34 is that their attack tools were hacked. The APT34, which has a significant cyber-espi-

[2] All of these logos, which represent the Iranian APTs, are works of FireEye.

onage capability, was hacked by the Russian in 2019. According to the joint report of the National Security Agency (NSA) of the USA and National Cyber Security Center (NCSC) of the UK that is affiliated with Government Communication Headquarters (GCHQ), Russia hacked the offensive cyber tools and the database of the APT34. In this respect, the Turla APT group, which is affiliated with Russian intelligence, has the cyber weapons of the APT34 that were used in the cyber operations, along with the database which includes information concerning the former actions. It is predicted that Russia has exploited these weapons and has conducted several operations, which are known to be done by APT34 (NSA, NCSC, 2019).

Image 8: APT34

Source: FireEye

d) APT35 (Phosphorus, Charming Kitten, Magic Hound, Ajax Security, Rocket Kitten, Saffron Rose, Cobalt Gypsy): The APT35 group, that is active in cyber espionage activities since 2013, targets academics and human right activists in general and aims at the defence, aviation, and energy sectors as well as the state institutions particularly. The majority of these targets live in Iran, the USA, Israel, and the UK and some others are in Turkey, France, Germany, Switzerland, UAE, India, and Denmark. The APT35 group, which works for IRGC, has recently carried out operations against the companies which work on the coronavirus vaccine. A cyberattack against the Gilead, that is, one of the companies, has been detected (Reuters, 2020). The group attacked through malicious emails that imitate journalists and sent to the top-level managers of the company. The level of the damage is unknown.

Some other attacks last year in April that targeted the World Health Organization (WHO) by the APT35 have also come forward. The group members aimed at the workers of WHO by introducing themselves as journalists or think tank employees through malicious emails that seem to be related to coronavirus (Bloomberg, 2020). In addition to email spear-phishing attacks, APT35 also operated a spear-phishing attack through SMS last December. The group draws attention with its remarkably intense activities (CERTFA, 2021).

The hacking of Home Box Office (HBO), the producer company of the Game of Thrones, was the first major operation of APT35, which also revealed some connections. According to the FBI reports, Behzad Mesri, who leaked the data concerning HBO, was a member of the Turk Black Hat hacker group. Several technical tools have been transferred to APT35 through this group. (ClearSky Cyber Security, 2017). APT35 has been using these tools ever since. Behzad Mesri is one of the four hackers who are associated with IRGC and wanted by the FBI. Furthermore, Behzad Mesri is one of the people to who Monica Witt has transferred information to. Monica Witt had worked in critical positions in the US Air Force Intelligence units until 2008 and turned out to be an IRGC spy in 2013 (FBI, 2019).

Image 9: APT35

Source: FireEye

e) APT39 (Chafer, Remix Kitten, TA454): APT39, active since 2015 and directly controlled by the Iran Ministry of Intelligence, targets especially Turkey, Israel, Saudi Arabia, UAE, and the USA. The group essentially conducts cyber espionage activities and specifically operates activities against energy, defence industry, telecommunication, and aviation companies. An attack campaign of the APT39 group that directly aimed at Turkey was detected in 2018. APT39 launched a cyber-espionage activity by leaking into the command control servers with malware through the website of Turkey Scholarships (turkiyeburslari.gov.tr), which is affiliated with the Presidency of Turks Abroad and Related Communities. The group has been attacking the public institutions in Turkey to get data from the users (Unit42, 2019). The scope of the damage to these activities is unknown.

Another noticeable characteristic of the APT39 group is its cyber espionage activities against Iran-centred addressed by developing a new operation tool. In other words, APT39 targets also the foreign diplomatic institutions in Iran (Kaspersky, 2019). Moreover, according to the researchers, there is a similarity between the operations of APT39 to the Middle Eastern countries and APT34 operations concerning attack methods, infrastructure, and timing. In fact, malware distribution methods, infrastructure systems, and targets of APT39 and APT34 overlap (FireEye, 2019). As noted in the second chapter, the APT39 group is also supported by the Rana Institute, which the Iran Ministry of Intelligence uses as a shell company.

Image 10: APT39

Source: FireEye

f) CopyKittens (Slayer Kitten): CopyKittens is a cyber espionage actor that is active since 2013 and targets primarily Israel, Saudi Arabia, and Turkey. It has also aimed at top-level officials in the United Nations (UN). CopyKittens targeted some companies and media institutions in Israel at first, then it has tended to more specific goals. Targeted institutions include state institutions like the Ministry of Foreign Affairs, academic research institutions, the defence industry sector, and major technology companies. The prominent targets seem to be Turkey and the Turkish Republic of Northern Cyprus (TRNC). According to the reports, Operation Wilted Tulip targeted the employees of the Ministry of Foreign Affairs both in Turkey and TRNC. The group sent malicious emails through the hacked email accounts to the relevant people. The document was likely stolen from a Turkish Ministry of Foreign Affairs employee and then exploited by threat actors (ClearSky, Trend Micro, 2017).

g) MuddyWater (Static Kitten, TEMP.Zagros, Seedworm TA450): MuddyWater is an APT group that has been active since 2017. It conducts intense cyber operations, particularly against Turkey, Saudi Arabia, and UAE. Russia and Pakistan are also stated to be the targets in some reports. MuddyWater APT group, which has increased its attacks against Turkey since 2018, is believed to be a cyber-espionage group that works for the Iranian government. The group operates its cyber espionage activities through create a backdoor besides spear-phishing. The group, which aims to get targets' data by advanced attack methods of social engineering, is known to imitate several institutions, including the Ministry of the Interior, General Directorate of Police, and Directorate General of Coastal Safety in Turkey, to attack with document-based malware (Kaspersky, 2018).

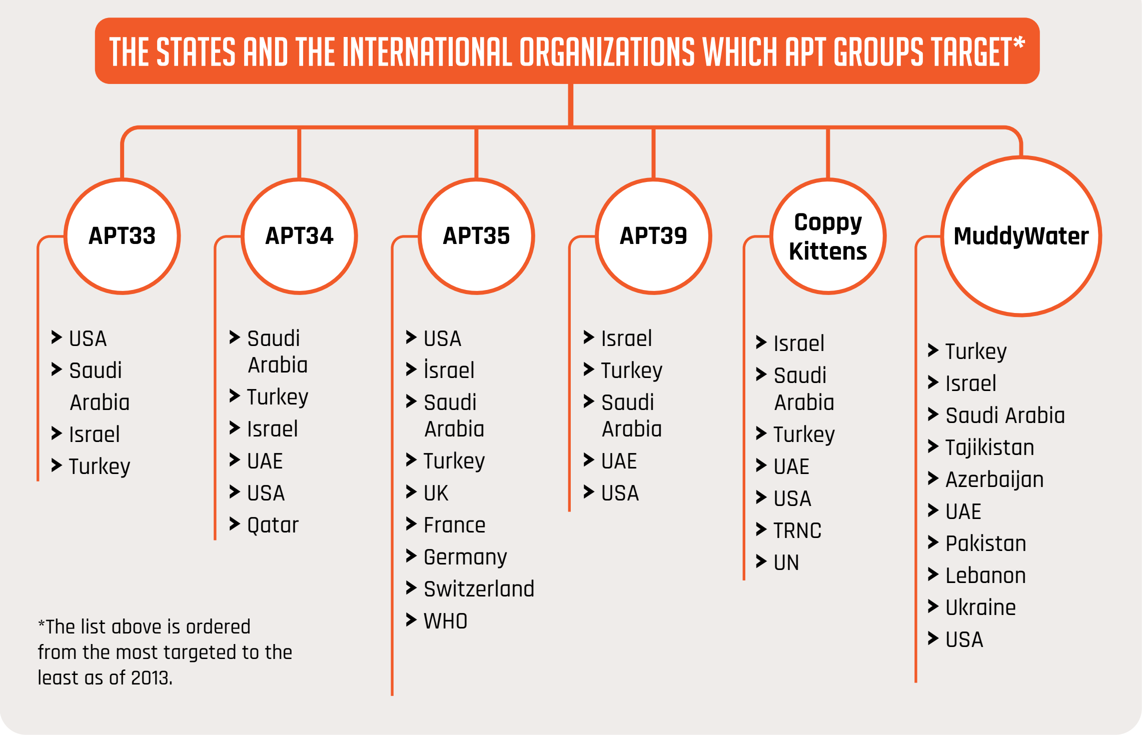
Another MuddyWater attack that targeted public institutions in Turkey was detected in 2019. The group imitated the Capital Markets Board of Turkey, in a word document that was written in Turkish for identity theft (CheckPoint, 2019). The level of damage of the attack is still unknown. Muddywater, unlike other ATP groups, also uses software vulnerabilities. In this context, the group operates against state institutions, telecommunication companies, and hundreds of companies in the energy and technology sectors (Symantec, 2018). This APT group allegedly works for IRGC, seems to focus on the states of the region, and continues its operations.

h) BlackShadow, Pay2Key, and Others: The hacker groups or hacktivists are the other dimensions of Iran's cyber threat actors. It is possible to mention ongoing hacking activities against Israel as a result of the tension between Israel and Iran. These groups conducts cyber operations by organizing in the digital platforms through the tags like "#OpIsrael". Even though they are not directly related to the Iran government, their activities are in line with the political interests of Tehran. The hacktivism activities of the groups have been intensified, especially after the assassination of Qasem Soleimani and Mohsen Fakhrizadeh. Their activities are mostly based on ideological motivations like the first phases of Ashiyane.

In the last years, especially since 2020, several different hacker groups have come forward. There is a rise in the number of attacks against Israel because of Iran-Israel tension, the assassination of Fakhrizadeh, and Mossad -attributed intelligence operations. The most prominent groups between them are BlackShadow and Pay2Key. BlackShadow had infiltrated into the intranet of Shirbit, which is the biggest insurance company in Israel, and started to leak a part of the sensitive data on forums and Telegram channels. The hackers, who demanded 1 million dollars of Bitcoin, continued to leak the data when the company did not accept their requests. The data that was shared in the Telegram included also the personal data of the company's CEO (Times of Israel, 2020). It was also noted that there was information about some of the personnel who work in critical state institutions in Israel.

Another attack against Israel was operated by Pay2Key. The group hacked Habana Labs company, which is established by Intel in Israel, at the first stage. Then, it succeeded to infiltrate Israel Aerospace Industries (IAI) and into Portnox, which is one of the biggest cybersecurity companies in Israel. The group that shared the data on

Image 11: The States and the International Organizations Which APT Groups Target



several different platforms of DarkWeb is predicted to consist of Iranian hackers (Siegal, 2020). According to the reports of cybersecurity specialists, the actor, which conducted these activities, is FoxKitten, and it has been active in the operations against Israel since June 2020 (ClearSky Cyber Security, 2020). The actors like Fox Kitten are expected to continue similar cyber attacks as a result of the ongoing Israel-Iran tension. There are concerns about the group to operate hacking activities also in 2021.

The organizations that are mentioned above do not represent the full list of Iran's cyber actors. The state-sponsored cyber actors in Iran or the hacker groups, apart from the mentioned actors, are known to be more than 20. The actors that are mentioned in this study are the most active operational groups, which have become a subject of analysis in many reports. There are also other APT groups that are less active or do not have any noticeable operational activity, such as Domestic Kitten and Pioneer Kitten.

Farzin Karimi, who allegedly forms hacker groups for Iran intelligence services like Behrooz Kamalian, should also be noted as a significant figure in Iran's cyber operations. Karimi has been involved in many cyber operations in the Ministry of Intelligence in Iran and played important roles in several attacks against other states. He continues his service to the Iran administration through Ravin Academy, which is believed to carry out cyber operations against Turkey last March and targeted the Ministry of Foreign Affairs and Ministry of National Defence (The Cyber Shafarat, 2020).

In conclusion, it is clear that there are many different cyber threat actors in Iran, and the majority of them are actively involved in cyber operations while others continue their activities in the control of the Ministry of Intelligence or IRGC. Moreover, most of Iran's cyber operations seem to be in the scope of cyber espionage or targeting critical infrastructures. Apart from these offensive cyber operations, it is also possible to mention Iran-originated information operations. Especially disinformation-oriented information operations on the online digital platforms may be categorized as a part of Iran's cyber operations.

3.2. Iran's Information Operations and the Other Activities

The facilities and capabilities that have emerged as a result of the development of technology create new domains for the states. The domain is the social media and other online platforms, as the subcategory of cyberspace, which is considered to be the fifth domain of the war. Several states conduct operational activities in these platforms through their technological potentials and capabilities.

Social media platforms come into prominence in this respect. The states, which involve in this sort of activity, are able to conduct information operations, especially on Twitter. It is also possible for these states to directly censor the targeted people or institutions. For instance, Saudi Arabia placed two spies on the Twitter company in November 2019 and it was revealed that the spies had targeted the users who post contents against Mohammed bin Salman and the Saudi administration and reported the users directly to the Saudi Intelligence Service (Newman, 2019).

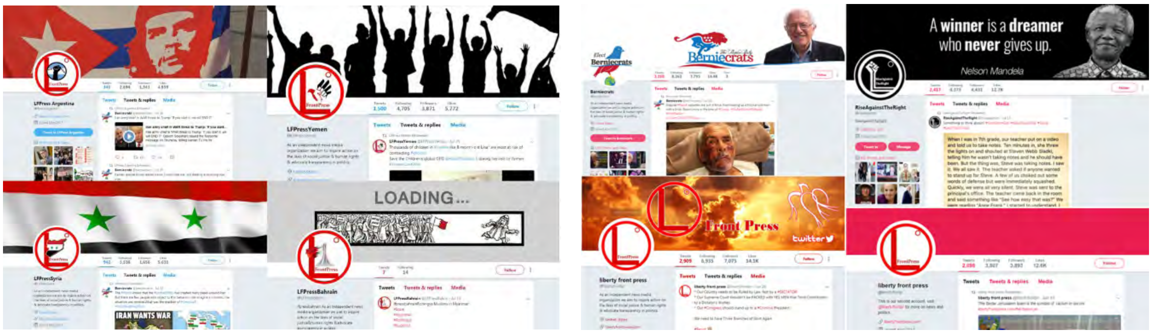
Iran is one of the states which pay attention to the information operations in the context of its interests. Iran, like China, Russia, and Saudi Arabia, uses its cyber actors for disinformation and misinformation activities, especially against the USA and Israel. The actors that are behind this sort of covered information operations are mostly state-sponsored institutions.

The hacker groups and the hacktivists, which are controlled by IRGC and the Ministry of Intelligence, are known to conduct information operations on Facebook, Instagram, and Twitter besides their cyberattack activities. Iran targets the opponent people or groups and tries to manipulate every anti-Iran news and the comments by organized groups.

Apart from the activities on social media, the other dimension of the operations is to create several websites in online platforms for pro-Iran and anti-Israel, and anti-US campaigns. Furthermore, there are some news websites that were specifically created for the US elections in the context of Iran's influence operations.

For instance, the FireEye report states that a state-sponsored information operation of Iran that targeted the US Presidential Election between 2017 and 2018 was detected. In this operation, there were some websites that were created to affect voter behaviour, such as Liberty Front Press, Instituto Manquehue, and The British Left. These websites matched with email domains that are registered in Iran. Furthermore, the report indicates that several numbers of Twitter accounts, which are associated with these websites, were also identified. Fake social media accounts that imitated American liberals and acted like to be supporters of Bernie Sanders were revealed in many social media applications along with Twitter. There were also websites and Twitter accounts that have published news about Yemen. Iran-based operational Twitter accounts that had targeted the Saudi administration, especially King Salman, with fake news, were also detected (FireEye, 2018).

Image 12: The Twitter Accounts That are Parts of the Information Operations



Source: FireEye

Apart from these operations, Iran also conducts digital propaganda and disinformation activities on social media. Facebook and Twitter are the two most prominent tools for Iran in these activities. It is possible to mention some Facebook pages concerning religious subjects that share pro-Khamenei content along with critical content against the states with which Iran has a conflict. For instance, a report of Digital Forensic Research Lab, which is affiliated with the Atlantic Council, states that Iran's disinformation-based information operations through Facebook and Twitter have been intensified between 2019 and 2020. These operations have become effective, especially on Instagram and Twitter after the assassination of Soleimani, and many pro-Soleimani posts have been detected. In the same period, several posts that targeted the US administration as well as Donald Trump, as the president of the era, were identified. These accounts are suspended by Twitter and Facebook (DFRLab, 2020).

According to the statements of Twitter and Facebook, thousands of Iran-based accounts have been suspended because of their information operation activities in the same period. Furthermore, Twitter has suspended the official accounts of the Supreme Leader Khamenei several times due to the complaints of Iranian users about censorship operations of the Iran administration through different hashtags.

The Iranian information operations started to focus on the US election from the mid-2020. The US Department of the Treasury declared that the five state-sponsored institutions of Iran are identified, which had attempted to affect the US election. According to the findings, the Iran administration targeted the election process to mislead the American voters by online disinformation activities. In the statement, Bayan Rasaneh Gostar Institute and International Union of Virtual Media, allegedly working for IRGC Quds Force, were reported to be the actors of the relevant operations. The institutions were claimed to target the US citizens by several publications in English concerning the election and the conspiracy theories about coronavirus (U.S. Department of the Treasury, 2020).

It is possible to argue that Iran continues its state-sponsored information operations, especially on social media. The applications such as Twitter, Facebook, and Instagram represent highly functional tools with their billions of users for the influence operations of the states like Iran. Iran's ongoing anti-US information operations are based on disinformation and misinformation. These activities on the digital ground will continue to be shaped by the interests of Tehran.

CONCLUSION

The cyber tools that are integrated with the technological elements are used intensively by states as a part of their military power. In addition to the cyberattacks that aim for intelligence gathering and damaging the critical targets, there are also information operations based on disinformation and misinformation. Sometimes, the propaganda activities come into prominence in these operations.

Iran is one of the states which conduct these operations for many years. Several state institutions or global companies that are experts in the field follow Iran's cyber operations closely. It is seen that Iran uses its offensive and defensive capabilities specifically against the USA, Israel, and Saudi Arabia because it conflicts with them.

The state-sponsored cyber threat actors in Iran carries out cyberattacks against the critical public institutions or companies of the relevant states through many different tools and methods. The APT groups and various hacker groups are known to play significant roles. Furthermore, state-sponsored Mabna Institute, Rana Institute, and Nasr Institute, along with the Ashiyane Security Group, which is involved in the activities secretly under the roof of these institutions, are the prominent cyber threat actors.

There have also been other structures like the Ashiyane Security Group, but according to the detailed analysis, it is possible to see a TTP-based development. The increasing number of cyber threat actors, which have been re-established with different names and improved their capacities and capabilities, act under the political interests of Tehran. They operate against "the primary targets" like the USA through cyber-espionage and destructive cyberattack activities.

The technical background and personnel of the organized groups, such as Ashiyane, Ajax, Cyber Fighters, are believed to form the most active APT groups in Iran that are APT33 and APT34. These APT groups represent Iran's operational cyber capability and the power of its "cyber army".

In some sources, moreover, Iran Cyber Army (ICA) is predicted to consist of these types of APT groups, the hackers that are associated with the Ministry of Intelligence and IRGC, cyber militias, and the shell companies that are mentioned above. When the operational cyber capabilities, the tools, the targets, and the TTP are examined, the overlapping between the possible structure and tools of the Iran Cyber Army and the relevant groups becomes obvious. Therefore, Iran Cyber Army can be understood as a code name to define all cyber actors who engage in offensive and defensive cyber organizations instead of a separate structure.

Iran's cyber capacity has significantly developed after the Stuxnet Operation. In the Shamoon Operation in 2012, Iran's capability to produce cyber weapons drew attention allegedly as the actor behind the operation. It also should be considered that Iran could produce/ develop the cyber weapon in cooperation with foreign actors like Russia.

It should also be emphasized that organizations such as institutes, companies, academic institutions, which educate hackers, are currently active. Additionally, according to the various technical reports that are examined in this study, it is possible to argue that the state-sponsored cyber organizations in Iran are directly controlled by IRGC or the Ministry of Intelligence. The information operations on the digital ground, including disinformation, misinformation, and propaganda, are also controlled and coordinated by the shell companies of these institutions or by the other official agencies.

Iran’s cyber policies, which are defined in terms of its interests, have been concerning for all regional and international actors along with its citizens. Iran, which targets many states, including the USA and Israel, has intensified specific cyber-attacks through its offensive cyber capability. Especially the APT groups, which are involved in cyber espionage activities, are seen as the most dangerous cyber threat actors by the states.

Iran originated cyber-attacks are concerning for Turkey as much as the USA, Israel, and Saudi Arabia. As stated in the study, an important part of Iran’s cyber operations has targeted Turkey. Due to the fact that cyber-espionage activities are not always detected, the scope of these attacks is not fully known. Still, considering the identified operational cyber activities that are analyzed in many reports, it is a fact that A specific target of Iran's cyber operations is Turkey.

In this context, the scope and the kind of potential damages that could be caused by Iran’s cyber threat actors according to the future of Iran-Turkey relations represent a crucial issue for Turkey. In fact, the probability of these kinds of cyber espionage operations should never be ignored, even if the relationship between the states is peaceful.

REFERENCES

- ARTICLE19. (2016). Tightening the Net: Internet Security and Censorship in Iran - Part 1: The National Internet Project. London: ARTICLE19.
- ARTICLE19. (2017). Tightening the Net - Part 2: The Soft War and Cyber Tactics in Iran. London: ARTICLE19.
- Bastani, H. (2012, December 13). Structure Of Iran's Cyber Warfare. Chaire Castex De Cyberstrategie Retrieved 2020, November 17 from https://tinyurl.com/rwnxctnr
- Bloomberg. (2020, May 7). Hackers Target WHO by Posing as Think Tank, Broadcaster. Bloomberg - Cybersecurity Retrieved 2020, October 22 from https://tinyurl.com/4r8h7hyh
- CERTFA. (2021, January 8). Charming Kitten's Christmas Gift. CERTFA - Blog Retrieved 2021, January 14 from https://tinyurl.com/4j7zjtst
- CheckPoint. (2019, April 10). The Muddy Waters of APT Attacks. CheckPoint - Research Retrieved 2021, January 14 from https://tinyurl.com/7kscncrp
- ClearSky Cyber Security. (2017). Charming Kitten. Tel Aviv: ClearSky Cyber Security.
- Clearsky Cyber Security. (2019). Iranian Nation-State APT Groups "Black Box" Leak. Tel Aviv: Clearsky Security Ltd.
- ClearSky Cyber Security. (2020). Pay2Kitten - Pay2Key Ransomware – A New Campaign by Fox Kitten. Tel Aviv: ClearSky.
- ClearSky, Trend Micro. (2017). Operation Wilted Tulip. Tel Aviv: ClearSky, Trend Micro.
- Collin Anderson, K. S. (2018). Iran's Cyber Threat: Espionage, Sabotage and Revenge. Washington: Carnegie Endowment for International Peace.
- Denning, D. (2017, December 12). Following the developing Iranian cyberthreat. The Conversation, Retrieved 2020, October 17 from https://tinyurl.com/469dmx3m
- DFRLab. (2020). Iranian Digital Influence Efforts. Washington: Atlantic Council.
- Esfandiari, G. (2020, September 4). RFERL. Iran To Work With China To Create National Internet System , Retrieved 2020, December 17 from https://tinyurl.com/5bw4e6ps
- Farivar, C. (2012, April 17). Security researcher unearths plans for Iran's halal Internet. ArsTechnica, Retrieved 2020, October 08 from https://tinyurl.com/56srnzc5
- FarsNews Agency. (2019, September 1). Iran's Security Systems Detect 29 Million Cyber Attacks Since May. FarsNews Agency, Retrieved 2020, December 14 from https://tinyurl.com/fvcp85tr
- FBI. (2018, March 23). Iranian Mabna Hackers. FBI, Retrieved 2020, November 28 from https://tinyurl.com/umsc3ry4
- FBI. (2018, March 23). State-Sponsored Cyber Theft - Nine Iranians Charged in Massive Hacking Campaign on Behalf of Iran Government. FBI, Retrieved 2020, December 30 from https://tinyurl.com/53tn93h3
- FBI. (2019, February 13). Former U.S. Service Member Charged with Espionage - American Woman Indicted Along with Four Iranian Cyber Criminals. FBI, Retrieved 2020, December 30 from https://tinyurl.com/6wxkjn7p

- FBI. (2020, September 17). FBI Releases Cybersecurity Advisory on Previously Undisclosed Iranian Malware Used to Monitor Dissidents and Travel and Telecommunications Companies. FBI - Boston, Retrieved 2021, January 11 from https://tinyurl.com/pp692t95
- Financial Tribune. (2016, August 26). Iran's National Information Network Launched. Financial Tribune, Retrieved 2020, October 16 from https://tinyurl.com/dbvtnzcw
- Fire Eye. (2014). Operation Saffron Rose. California: FireEye Corp.
- FireEye. (2017, eptember 20). Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. FireEye - Threat Research, Retrieved 2020, December 27 from https://tinyurl.com/vn2xny9n
- FireEye. (2018). Suspected Iranian Influence Operation. California: FireEye Inc.
- FireEye. (2019, January 29). APT39: An Iranian Cyber Espionage Group Focused on Personal Information. FireEye - Threat Research, Retrieved 2020, December 24 from https://tinyurl.com/k5xbtnpv
- Hassold, C. (2018, March 26). Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment. PhishLabs, Retrieved 2020, December 28 from https://tinyurl.com/ypfte684
- IranWire. (2019, April 10). Cyberspace Institutions and The Physical Training Organization of the Basij. IranWire, Retrieved 2020, October 24 from https://iranwire.com/en/features/5739
- IranWire. (2019, April 10). The Organization for the Mobilization of the Oppressed. IranWire, Retrieved 2020, November 27 from https://iranwire.com/en/features/5744
- Islamic Parliament Research Center of The Islamic Republic of Iran. (2012, January 12). Approval of the Supreme Council of Cyberspace regarding the duties, powers and members of the Supreme Commission for Cyberspace Security. Islamic Parliament Research Center of The Islamic Republic of Iran, Retrieved 2020, December 19 from https://rc.majlis.ir/fa/law/print_version/821931
- Islamic Republic of Iran Ministry of I.C.T. (2010, January 10). A glance to the national Internet in the current 4 years. Information and Communications Technology Ministry, Retrieved 2020, October 20 from https://tinyurl.com/anza3wav
- Islamic Republic of Iran Ministry of I.C.T. (2011, December 21). Head of Iran IT Organization: 40 articles related to ICT development in the fifth development plan. Ministry of Information and Communications Technology, Retrieved 2020, October 19 from https://tinyurl.com/p6au2ry8
- Islamic Republic of Iran Ministry of I.C.T. (2015, June 13). Dr. Vaezi meets Head of Chinese Cyberspace Administration. Ministry of Information and Communications Technology of Iran, Retrieved 2020, October 19 from https://tinyurl.com/w24xnb6z
- Kaspersky. (2018, October 10). MuddyWater expands operations. Kaspersky - Securelist, Retrieved 2020, December 27 from https://securelist.com/muddywater/88059/
- Kaspersky. (2019, January 30). Chafer used Remexi malware to spy on Iran-based foreign diplomatic entities. Securelist - Kaspersky, Retrieved 2020, December 30 from https://tinyurl.com/dpnnvbpc
- Kim Zetter, H. M. (2019, September 2). Yahoo News. Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran: https, Retrieved 2020, October 04 from//tinyurl.com/uwb2mhdv
- Newman, L. H. (2019, November 6). Twitter Insiders Allegedly Spied for Saudi Arabia. WIRED: https, Retrieved 2020, October 10 from//www.wired.com/story/twitter-insiders-saudi-arabia-spy/
- Nicolas Falliere, L. O. (2010). W32.Stuxnet Dossier. ABD: Symantec.

- NSA, NCSC. (2019). Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims. US, UK: NSA, NCSC (v1).
- Open Research Network. (1999). Iran's Telecom and Internet Sector: A Comprehensive Survey. U.S.: The Open Research Network.
- Recorded Future - CHRIS. (2013, January 2). Deconstructing the Al-Qassam Cyber Fighters Assault on US Banks. Recorded Future, Retrieved 2021, January 12 from https://tinyurl.com/rcdam26j
- Recorded Future - Insikt Group. (2019). Iranian Threat Actor Amasses Large Cyber Operations Infrastructure Network to Target Saudi Organizations. Washington: Recorded Future - CTA-2019-0626.
- Recorded Future - Insikt Group. (2019, January 16). The History of Ashiyane: Iran's First Security Forum. Recorded Future, Retrieved 2020, October 28 from https://www.recordedfuture.com/ashiyane-forum-history/
- Recorded Future - Insikt Group. (2020). Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure. Washington: Recorded Future (CTA-IR-2020-0409).
- REFWorld. (2015, January 16). Iran: Government surveillance capacity and control, including media censorship and surveillance of individual Internet activity. REFWorld, Retrieved 2020, October 17 from https://www.refworld.org/docid/550fdcc34.html
- Reuters. (2020, May 8). Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources. Reuters, Retrieved 2020, December 25 from https//tinyurl.com/23s6bwu2
- RISKIQ. (2020, December 2). Shadow Academy: Hiding in the shadows of Mabna Institute. RiskIQ, Retrieved 2021, January 14 from https//community.riskiq.com/article/44eb0802
- Samii, B. (2006, September 29). Iran: Government Strengthens Its Control Of The Internet. RFERL, Retrieved 2020, October 18 from https://www.rferl.org/a/1071706.html
- Siegal, T. (2020, December 25). Iranian hackers strike again, target Israeli cyber-security firm Portnox. The Jerusalem Post, Retrieved 2021, January 10 from https//tinyurl.com/yjec22pw
- sKyWIper Analysis Team. (2012, May). sKyWIper (a.k.a Flame a.k.a Flamer): A Complex Malware for Targeted Attacks. Crysys Retrieved 2020, November 04 from https://www.crysys.hu/publications/files/skywiper.pdf
- Small Media. (2019, February 22). Iran's Cyber Police—'Society-Based Policing' and the Rise of Peer Surveillance. Small Media Retrieved 2020, November 13 from https://tinyurl.com/n8dzpx2v
- SmallMedia. (2017, September 25). Filterwatch // August 2017. Small Media Retrieved 2020, December 10 from https://smallmedia.org.uk/news/filterwatch-august-2017
- Spadoni, G. (2019). IRGC Cyber-Warfare Capabilities. Herzliya-Israel: International Institute for Counter-Terrorism - IDC Herzliya.
- Stecklow, S. (2012, March 22). Special Report: Chinese firm helps Iran spy on citizens. Reuters. Retrieved 2020, December 18 from https://tinyurl.com/23f5ed5n
- Symantec. (2011). W32.Duqu: The Precursor to the Next Stuxnet. V. 1.4. Symantec Security Response.
- Symantec. (2018, December 11). Seedworm: Group Compromises Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms. Symantec - Threat Intelligence Retrieved 2020, December 17 from https://tinyurl.com/77mwa4ad

- Symantec. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S. Symantec - Threat Intelligence Retrieved 2021, January 11 from https://tinyurl.com/uxtfyehv
- Tabansky, L. (2018). Iran's Cybered Warfare Meets - Western Cyber Insecurity. F. Rugge içinde, Confronting An "Axis of Cyber?" (s. 131). Milano: ISPI.
- Tehran Times. (2019, May 8). Hotgram, Talagram to be appeared as independent apps: official. Tehran Times Retrieved 2020, November 21 from https://tinyurl.com/y24d2rce
- Tehran Times. (2019, February 16). Tehran Times. National optical fiber network to expand by 20% to 84,000km Retrieved 2020, October 27 from https//tinyurl.com/yzw26uuz
- The Cyber Shafarat. (2020, May 12). Farzin Karimi Moves From Pure MOIS to Ravin Academy. Treadstone 71 - The Cyber Shafarat Retrieved 2021, January 12 from https://cybershafarat.com/2020/05/12/farzin-karimi/
- Times of Israel. (2020, December 3). Hackers who breached Israeli insurance firm demand $1m to keep data private. Times of Israel Retrieved 2021, January 14 from https://tinyurl.com/39y2t7h2
- U.S. Department of State. (2020, September 17). The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry. U.S. Department of State Retrieved 2020, December 29 from https://tinyurl.com/hunur8ph
- U.S. Department of the Treasury. (2018, January 12). Treasury Sanctions Individuals and Entities for Human Rights Abuses and Censorship in Iran, and Support to Sanctioned Weapons Proliferators. U.S. Department of the Treausry Retrieved 2020, December 19 from https://home.treasury.gov/news/press-releases/sm0250
- U.S. Department of the Treasury. (2020, October 22). Treasury Sanctions Iranian Entities for Attempted Election Interference. U.S. Department of the Treasury Retrieved 2021, January 14 from https://home.treasury.gov/news/press-releases/sm1158
- Ungerleider, N. (2012, February 23). Iran's "Second Internet" Rivals Censorship Of China's "Great Firewall". FastCompany Retrieved 2020, October 18 from https://tinyurl.com/bxnaf74
- Unit42. (2019, March 4). New Python-Based Payload MechaFlounder Used by Chafer. PaloAlto Networks - Unit42 Retrieved 2020, November 16 from https://tinyurl.com/mhyy8daw

Notes

Notes

İRAM
YAYINLARI

About İRAM

Due to its historical depth and material power, Iran is among the countries that have to be reckoned with in the domain of international relations. The deep-rooted historical relations between Iran and Turkey, border-sharing, and comprehensive business relations makes it necessary for Turkey to understand Iran in a multitude of ways. Based on this necessity, the Center for Iranian Studies (İran Araştırmaları Merkezi, İRAM) was established as an independent think tank in Ankara with the purpose of informing the Turkish public and interested parties about Iran. With this in mind, not only does İRAM produce field research, reports, and analyses based on primary resources, it also provides language courses, internships/scholarship programs, support for projects and graduate theses, workshops, and expert seminars in order to meet the need for experts and researchers on Iran in various disciplines in Turkey. Offering a platform where academicians can share their research on Iran, İRAM also provides digital and printed publications on a wide variety of topics ranging from economy to domestic politics, international policy to security, and Shi'ism to society and culture.

İRAM
Center for Iranian Studies in Ankara

ANKARA
Oğuzlar, 1397. St. No: 14
06520, Balgat, Çankaya, Ankara, Turkey
Phone: +90 312 284 55 02 - 03
Fax: +90 312 284 55 04
e-mail: info@iramcenter.org
www.iramcenter.org

İSTANBUL
Üst Zeren St, No: 40
Levent, Beşiktaş, İstanbul, Turkey
Phone: +90 212 264 35 81 | +90 212 268 33 00
Fax: +90 212 264 35 18
e-mail: iramistanbul@iramcenter.org
www.iramcenter.org