İRAN'IN SİBER GÜVENLİK STRATEJİSİNİN SALDIRI VE SAVUNMA KAPASİTESİ BAKIMINDAN ANALİZİ

Article *in* Turkish Studies - Social Sciences · January 2019

DOI: 10.29228/TurkishStudies.22799

1 author:

Ali Burak Darıcılı

35 PUBLICATIONS **21** CITATIONS

SEE PROFILE

Turkish Studies
Social Sciences
Volume 14 Issue 3, 2019, p. 409-425
DOI: 10.29228/TurkishStudies.22799
ISSN: 2667-5617
Skopje/MACEDONIA-Ankara/TURKEY

INTERNATIONAL BALKAN UNIVERSITY
EXCELLENCE FOR THE FUTURE
IBU.EDU.MK

Research Article / Araştırma Makalesi

Article Info/Makale Bilgisi

Received/Geliş: 04.02.2019 Accepted/Kabul: 10.06.2019

Report Dates/Rapor Tarihleri: Referee 1 (15.03.2019)-Referee 2 (11.03.2019)- Referee 3 (18.03.2019)

This article was checked by iThenticate.

ANALYSIS OF IRAN'S CYBER SECURITY STRATEGY WITH REGARD TO THE ATTACK AND THE DEFENSE CAPACITY

Ali Burak DARICILI[*]

ABSTRACT

The Stuxnet Virus was released in June 2010 and has affected Iran's nuclear facilities in Bushehr and Natanz. It was claimed that the United States of America (USA) and Israel secret services together have a role in the planning of this cyber-attack. Following this cover activity, also known as Operation Olympic Games in the literature, Iran considered the need to take serious measures in the field of cyber security and aimed to reach an effective cyber security capacity in cyber space with the investments made in 2010.

As it is seen, Iran's plans to develop a cyber security strategy were realized within the scope of an action-reaction relation through a retaliation reflex after the mentioned attack to the nuclear facilities. Nevertheless, Iran's efforts to improve its cyber security capacity, which began with a motivation for retaliation in the first place, turned into a goal to make Iran a strong actor in cyberspace with the measures taken in the following periods.

On the other hand, Iran has serious efforts to improve its cyber security strategy especially in terms of attack. One of the most important reasons for this is that Iran has a low level of technology development and use. More precisely, the fact that a significant part of critical infrastructure is still controlled by mechanical technologies provides Iran a natural advantage in terms of cyber defense. Iran, which has started to invest in the cyber-attack capacity instead of defense after 2010 with this advantage, has achieved its effective position in cyberspace today.

As a result, it can be argued that Iran has introduced more serious plans in the field of cyber security than in the past after Stuxnet Attack.

[*] Dr. Faculty Member Ali Burak Darıcılı, Bursa Technical University, Faculty of Humanities and Social Sciences, International Relations Department, E-mail; ali.daricili@btu.edu.tr

In our article, the cyber security strategy of Iran which has a rapidly developing cyber-attack capacity and the institutional structures that play a role in this strategy with the steps taken after the Stuxnet Attack will be analyzed. In addition, the alleged cyber-attacks conducted by Iran will be discussed as well.

STRUCTURED ABSTRACT

Iran has been striving to improve its capacity for cyber-attack and defense following the Stuxnet Virus attack in June 2010 that affected nuclear facilities in Bushehr and Natanz. On the other hand, it was claimed that the United States of America (USA) and Israel secret services together have a role in the planning of this cyber-attack. Following this cover activity, also known as Operation Olympic Games in the literature, Iran reached an effective cyber security capacity in cyber space with the investments it made.

As is seen Iran's plans to develop its cyber security strategy started with a motivation of retaliation against the US and Israel in the first place. Nevertheless, Iran's efforts to improve its cyber security capacity, turned Iran into a strong actor in cyberspace in terms of cyber-attack capacity with the developments made in the following periods.

Besides, it can be argued that Iran has introduced more serious plans in the cyber security field than in the past. It is also evident that the cyber-attack capacity is rapidly evolving along with the steps taken after the Stuxnet Attack. These claims will be better understood by analyzing Iran's cyber security strategy and the institutional structures involved in this strategy, as well as by examining the alleged cyber-attacks carried out by Iran.

As can be seen, Iran has a national aim to have a strong cyber-attack capacity. Benefitting from the asymmetric advantages provided by the cyber space in the struggle of power especially against the USA, Saudi Arabia and Israel in the Middle East is the desire of Iran, which is not a global power, essentially at the background of the target in question. In this respect, Iran does not refrain from power struggle with the USA in cyber space in a cost efficient and riskless manner and through hiding its source by benefitting from the advantages of cyber space despite it is far weaker than the USD both in terms of conventional power and technological power with the measures it has taken after 2010.

The development of information technology, most of information becomes important for the institution at low or high level which should be protected from physical and cyber threats (Ateş vd., 2017). This is one of the basic reason for why Iran plans to estanlish a strong cyber-attack capacity. Another reason why Iran wants to increase the capacity of the cyber-attack is that it wants to establish deterrence for the cyber-attacks to be carried out by the USA, Israel or other hostile countries as in the Stuxnet Attack case. It is also clear that having an effective cyber-attack capacity will provide military deterrence against any conventional attack likely to be carried out against Iran in the future.

In the context of the effective activities of such organizations, Iran has become a concrete example of how a state with weak military in the

international system can reach an effective cyber-attack capacity. The fact that Iran is underdeveloped in terms of developing technologies and using them compared to USA and Israel, which Iran is in competition regarding cyber defense capacity, also provides some important advantages. The fact that a significant part of the Iranian critical infrastructure is still controlled by mechanical technologies provides Iran a natural advantage in terms of cyber defense. For this reason, Iran attached importance to actions towards controlling internet and social media which are the basic media where the opponent movements are organized instead of protecting the critical infrastructure from cyber-attacks in its cyber defense strategy.

It is understood that there are internal and external targets of the cyber-attacks claimed to be carried out by Iran. It is seen that the focus of foreign targets are mainly the USA, Israel and Saudi Arabia, where Iran is having problems in foreign policy, while internal targets are composed of opposition structures. Internal targets are government officials, reformist politicians, media workers, local religious leaders, religious minorities, cultural figures and anti-regime terrorist organizations, various groups and separatist movements that tend to fractionize within the regime.

On the other hand, Iran's internal and external defense priorities can be summarized as protection of the regime and the integrity of the country which has an heterogenous social structure, preservation and development of the Iranian Society and the Shiite heritage and presence in the Middle East region, to have the regional power role, to take an advantage over the states and groups perceived as regional threats, to increase its effectiveness in the struggle for regional leadership, the desire to struggle with external interventions targeting the integrity and political independence of the country. In this context, it can be seen that Iran's targets for cyber-attacks are determined in accordance with Iran's traditional internal and external defense priorities.

As a result, it can be stated that the Iranian cyber capacity has started to develop rapidly with the planning and investments made after 2010 in terms of defense and attack. However, the embargo imposed on Iran and the isolation of the country from the international system prevent Iran from developing a cyber-attack capacity with technologically more sophisticated means. In addition, cyber capacity of Iran is in need of foreign aid and cannot bring its effectiveness to a more professional level.

It can also be stated that Iran will endeavour to improve the possibilities and capabilities of cyber-attacks with proxy organizations by supporting the cyber capacity of close groups such as the Yemeni Cyber Army, the Syrian Electronic Army and Hezbollah. Iran is already trying to effectively benefit from the proxy organizations in its current cyber-attack strategy. In this context, it is possible that Iran will further develop its proxy cyber-attack system with new investments.

It can also be pointed out that the brain drain from Iran to Western countries for seeking a better life is an important obstacle for Iran to develop an efficient cyber capacity. In this context, it is estimated that about 150 thousand people with skilled labour migrate from Iran every year, and that the cost of this migration to Iran is about 150 billion

dollars. In this respect, it is clear that the Iranian government will have serious difficulties in establishing an effective cyber security capacity if it fails to keep the qualified work force in the country.

Keywords: Iran, Stuxnet Virus, Cyber Space, Cyber Attack, Cyber Defense

İRAN'IN SİBER GÜVENLİK STRATEJİSİNİN SALDIRI VE SAVUNMA KAPASİTESİ BAKIMINDAN ANALİZİ

ÖZ

Stuxnet Virüsü, Haziran 2010 yılında açığa çıkmış ve İran'ın Buşehr ve Natanz'daki nükleer tesislerini etkilemiştir. Bu siber saldırının planlanmasında Amerika Birleşik Devletleri (ABD) ve İsrail gizli servislerinin birlikte rol oynadıkları iddia edilmiştir. Literatürde Olimpiyat Oyunları Operasyonu (Operation Olympic Games) olarak da bilinen bu örtülü faaliyet akabinde İran, siber güvenlik alanında ciddi tedbirler alması gerektiğini anlayarak, 2010 yılı sonrası yaptığı yatırımlar ile birlikte siber uzayda etkili bir siber güvenlik kapasitesine ulaşmayı hedeflemiştir.

Görüldüğü üzere İran'ın siber güvenlik stratejisini geliştirmeye yönelik planlamaları, nükleer tesislerine yönelik söz konusu saldırı sonrasında bir etki-tepki ilişkisi kapsamında misilleme refleksi ile gerçekleşmiştir. Bununla birlikte ilk etapta bir misilleme motivasyonu ile başlayan İran'ın siber güvenlik kapasitesini geliştirmeye yönelik gayretleri, ilerleyen dönemlerde alınan tedbirlerle İran'ı siber uzayda güçlü bir aktör haline getirme hedefine dönüşmüştür.

Öte yandan İran siber güvenlik stratejisini özellikle saldırı yönünden geliştirme noktasında ciddi gayret sarf etmektedir. Bunun en önemli nedenlerinden biri İran'ın teknoloji geliştirme ve bunu kullanma noktasında düşük seviyede olmasından kaynaklanmaktadır. Daha net bir ifadeyle kritik altyapılarının önemli bir kısmının hala mekanik teknolojiler ile kontrol ediliyor olması, İran'a siber savunma yönünden doğal bir avantaj sağlamaktadır. Bu avantajı ile birlikte savunmadan ziyade siber saldırı kapasitesine 2010 yılı sonrasında yatırım yapmaya başlayan İran, siber uzayda günümüzdeki etkili konumuna ulaşmıştır.

Sonuç olarak, Stuxnet Atağı akabinde İran'ın siber güvenlik alanında geçmişe kıyasla daha ciddi planlamalar ortaya koyduğu iddia edilebilir. Bu iddia kapsamda makalemizde Stuxnet Atağı sonrasında atılan adımlar ile birlikte özellikle siber saldırı kapasitesi hızla gelişen İran'ın siber güvenlik stratejisi ve bu stratejide rol oynayan kurumsal yapılanmaları analiz edilecek, ayrıca İran tarafından gerçekleştirildiği iddia edilen siber ataklar irdelenecektir.

Anahtar Kelimeler: İran, Stuxnet Virüsü, Siber Uzay, Siber Saldırı, Siber Savunma

1. Introduction

The definitions related to cyberspace, display major differences. The common ground of these methaphorical definitions and abstractions, points out the network that are connected to each other via the possibilities of internet based technologies. In this context, cyberspace can be defined as *"a digital area that is designed by human and that is connected to each other via internet based technologies".* On the other hand, the mentioned cyber area is considered as a possibility for developing their military capacity, namely hard power, by nations that are in international system (See more at; Darıcılı, 2017: 1-3). In this sense, nations put forward various plans and make high budget investments in order to be effective in cyberspace. When the facts that cyberspace because of its nature, asymetrises the threats and makes the sources and timings unknown, are taken into consideration, it can be claimed that all these competion processes, within the real political paradigms, deepen the power wars among the nations in international system, increase the ambiguities and conflict possibilities in international system and thus, make the international system less reliable than previous periods. Iran has started to try her hardest in terms of developing the capacity cyber attack via the means of cyberspace, upon the attacks to Buşehr and Natanz by Stuxnet Virus in June 2010, which was claimed to be planned by Iran, USA and Israel.

In 2001, the first censoring precautions have been put into application by Culture Revolution High Council (Shorā-ye Enghelāb-e Farhangi). In 2003, the first opponent blogger of Iran, Sina Motalebi, was arrested. In 2005, upon election of Mahmoud Ahmedinejad as the president, the precautions of Iran towards internet access have gained pace (Anderson and Sadjadpour, 2018: 9).

The social/communal movement, namely Green Movement, which started with the reformist claims of Iranian people that do not accept the June 2009 elections because of the oppressive policies of Ahmadinejad, caused crucial political and social results in Iran (Kamacı, 2013). The cyber defense strategy of Iran have started to be structured to an important extent with the effect of political and social results of the Green Movement. In this context, the fact that the masses organized via social media during the Green Movement, caused Iranian regime to develop necessary precautions. Therefore, serious precautions towards internet usage and access to the social media have started to be applied in Iran (Anderson and Sadjadpour, 2018: 10).

The attacks to the nuclear institutions in Buşehr and Natanz in 2010 via Stuxnet virus, played the major role in defining the Iran's cyber security strategies of today. From that date on, Iran have started to put forward serious plannings by both empowering its cyber defense and developing its cyber attack capacity, which was accepted as main target.

As a result, it can be argued that Iran has a professional and sophisticated plan in the field of cyber security. In this article, the details of the Stuxnet Attack, the steps taken by Iran to control the internet, the institutional structures that play a role in Iran's cyber security strategy and the cyber-attacks that were planned by Iran will be analyzed to determine the validity of this claim.

2. Cyber Defence Strategy Of Iran And The Control Of Internet

The fact that the social movements of Green Movement were organized via social media and the attacks to Iranian nuclear institutions in 2010, caused crucial results in terms of Iran's cyber defense strategies. As it is afore mentioned, the fact that an important majority of Iran's critical infrastructure are still controlled by mechanical control systems, create a natural advantage to Iran in terms of cyber defence. Therefore Iran, have started to give importance to control the internet and social media, which are the sources of anti-regime movements, instead of giving importance to protecting critical infrastructure from cyber attacks in cyber defense strategies.

In this frame, 27% of internet web sites that were active in 2012 were banned and the 50% of 500 web sites that were popular in almost all the countries in the world were blocked in Iran in 2013. In addition to YouTube, Facebook, Twitter and Google Plus; health, science, sport and shopping sites were

among the banned websites. As a result of all these applications, there emerged a boom in the usage of VPN (Virtual Private Networks) in Iran (Small Media, 2018).

In addition to all these evolutions Iran, she increased her efforts in banning the internet sites that were seen as prejudicial in 2010, via the filter applications that she started to buy in 2006. Another move that Iran made in order to control the internet was to slow down the pace of the internet before or during the important events. For example, during the elections of 2013 this method is applied (Small Media, 2018). For the events that happened in various countries during Arab Spring, the same method was used as well (Iran's News Update, 2014). During the communal movements in 2017-2018, Iranian government banned access to mobile phones, internet and to the applications such as Instagram and Telgram (CNN, 2017).

The efforts towards the idea of structuring her own national internet that emerged in 2010, went up to an important level in 2012. In 2012 approximately 10.000 computers that were obtained from private and public sectors, were included to the alternative internet system, namely Halal Internet. (American Foreign Policy Council, 2013). In August 2016, Iran Information Technologies Minister Mahmoud Vaezi, declared to the press that *Iran completed the first level of planning an internet system that is appropriate for Islamic criteria, fast, reliable and cheap* (BBC, 2016). The plannings that are in the scope of mentioned first level, developed vi inclusion e-government systems and national web pages to the national internet system.

In 2011 Iran, established a Cyber Command by staying connected with Revolution Protectors. Furthermore, Computer Emergency Response Team Centre (MAHER) is founded, again by staying connected with the mentioned corporations, in order to detect and deactivate the cyber attacks towards Iran. Besides, a cyber defence programme was scheduled and the efforts to develop anti-virus programmes gained pace in Imam Hossein University (IHLS, 2013). It is also brought forward that Islamic Revolution Protectors follow technically the communication in Iran that is run by social media applications such as Facebook, Viber and WhatsApp, via an internet supervision system called Operation Spider (or Project Spider) (Reuters, 2015).

In December 2012, Iran established a social media platform called "Mehr", as an alternative to YouTube. In this context, in the mentioned date the Iranian authorities claimed that they would continue to establish social media applications that would act as alternatives to Facebook and Twitter (American Foreign Policy Council, 2013).

Furthermore, Iran's target towards developing its cyber attack capacity, constitutes an appropriate strategy with her foreign policy priorities. Iran's foreign policy mainly structures around the principles of protecting the regime and integrity and political independency of the country that is heterogenious, protecting and developing the Iranian society and Şii heritance in the Middle East region and providing regional power role (Efegil, 2012: 63). In this context, Iran aims at gaining competitive advantage against nations and groups in the region that are considered as threat, via a powerful cyber capacity, increasing her effectiveness in the struggle for regional leadership and struggling with external interventions that target at political independency and country integrity.

In this sense, evaluating the details of Olympic Games Operation, which is the main motivation of Iran's increasing her cyber attack capacity and which gained awareness seriously to the regime in terms of cyber security, constitute great importance for this study, before analysing Iran's cyber attack capacity and the structures that play role in this capacity.

2. Stuxnet Virus And Olympic Games Operation

The cyber attacks that were claimed to be planned by the USA and Israel secret services in 2010 to Iranian cities Buşehr and Natanz, via a virus named Stuxnet (Olympic Games Operations), constituted an identifying role in Iran's cyber attack strategy structure. After the mentioned date, Iran developed an

agressive cyber attack strategy that does not refrain from arranging cyber attacks towards nations and groups that are considered as threat via plannings and tried to gain an effective cyber attack capacity in cyber space.

In the context of mentioned cyber attack, Iran's nuclear institutions were physically damaged and thus, the continuance of Iran's nuclear programme was delayed. As it can be understood, "Stuxnet" is a cyber weapon that was developed to attack Iran's nuclear institutions and that was realised in June 2010. Although this attack was not undertaken officially by any country, in the background of the attack there was most probably a secret activity that wass based on the USA-Israel colloboration and there have not been any contradiction from both countries about these claims yet (Darıcılı, 2017: 104) .

About the subject, in some news in the USA press it was claimed that Stuxnet was developed in National Security Agency (NSA) in Maryland, with the coordination of Central Intelligence Agency (CIA) and with the command of Obama and tested in a model nuclear institution founded in Israel (Sanger, 2011). On the other hand, via an Iranian attendant that worked in the mentioned nuclear institutions and most probably engaged by Israel Secret Service (MOSSAD), targeted at damaging enrichment processes of centrifuges, which are used for enriching uranium, by effecting their turning pace and thus, decreasing their exposure time (Darıcılı, 2017: 105). He also succeded in deceiving the engineers by turning the 21 second screenshot that he took before. He increased and decreased the turning paces of centrifuges and decreased their exposure time at the background. Because of the fact that the damaged centrifuges were not replaced, the mentioned sabotage caused an explosion. As a result, although Iran's nuclear enrichment process did not completely finished, there happened a delay of 1-2 years (Cyber Bulletin, 2014).

Stuxnet, should be evaluated as an attack case because of the fact that it caused precursors in various work fields. In this context, the fact that industrial control systems that are closed to the external world can be targets to the sophisticated softwares together with Stuxnet, in terms of cyber security studies. This attack, in terms of international relations discipline, constitutes importance as it shows that how cyber attack methods can be used as a way to make pressure and force in foreign policy.

In the scope of this study, the mentioned attack that targeted at Iran's nuclear institutions constitutes great importance because of the fact that it causes an awareness among the actors that manage national system in the field of cyber security. In this frame, Iran has started to develop plans in order to reach a powerful attack capacity in the scope of mentioned foreign policies and today, she has reached to a point to be evaluated as the third cyber threat focus in the cyber space for the USA after Russia and China (For further information; Slavin and Healey, 2013: 1-8).

In this context there is important information related to Iran's cyber capacity, which is considered as the third threat focus after Russia and China in the USA's cyber security centers, in the document named "The Department of Cyber Strategy".In the mentioned document, which was accepted in 23 April 2015, it is pointed out that Russian Federation and China have developed a quite advanced cyber capacity and strategy. In this context, Russia's cyber power is defined as *"very difficult to detecet and deciphre"*. On the other hand China is accused of planning cyber espionage operations towards stealing the USA's intellectual entity. In this document Iran is mentioned as although she has a relatively limited cyber capacity when compared to China and Russia, necessary precautions have to be taken towards her in order to protect the USA and the national interests (The Department of Defence of the USA, 2015: 9). On the other hand, it should not be forgatten that the USA, who evaluates Iran as the third most effective cyber threat focus, is the most important global cyber power that dominates cyber space together with Russia and China (Darıcılı and Özdal, 2017: 121).

The structures that have role in Iran's cyber space, on the other hand, are organized as complex and integrated layers. These settlements, contain formal and informal corporations and serve to the Iran's target of developing an effective cyber attack strategy in the scope of their responsibility fields.

4. Formal And Informal Corporations That Take Place In Iran's Cyber Capacity

Iran, has started to construct various formal and informal settlements that develop her cyber attack capacity via the precautions that were taken after 2010. Cyber Security High Council (Shoray-e Aali-e Fazaye Majazi) is the most important of these settlements. The council, which was founded with the instruction of Ayatollah Khamenei in March 2012, makes deterministic decisions about Iran's cyber defence and attack capacity (BBC Persian, 2018: 1). In this context, Cyber Security High Council can be evaluated as a framework settlement that shapes Iran's cyber security strategy.

Cyber Security Commandership (Gharargah-e Defa-e Saiberi), was found in November 2010. This commandership, acts under the control of Iran's passive Civil Defence Organization (Sazeman-e Padafand-e Gheyr-e Amel). Cyber Security Commandership is responsible of providing the security of the country and the critical infrastructures towards cyber threats. The mentioned commandership, which acts towards providing the country's cyber defence capacity as it was defined in its foundation process, has today evolved into a structure that mostly serves to the aim of controlling opposition factors in Iran (BBC Persian, 2018: 2).

An informal settlement that is called as Iranian Cyber Army, constitutes great importance in structuring Iranian cyber attack capacity. In this settlement, Iranian nationalists volunteer civil citizens and hackers take place. It is also claimed that Iranian Cyber Army is supported and financed by Iranian Revolution Protectors (Sepâh-e Pâsdârân-e Enghelâb-e Eslâmi) and Iranian Intelligence Ministry (Vezarat-e Ettela'at Jomhuri-ye Eslami-ye Iran) (For further information; BBC Persian, 2018: 2-3). In this sense, in Iranian Cyber Army there are local universities and individuals that grow up in amateur hacker groups and take role unofficially in Islam Revolution Protectors by getting communicated to them in the period (Anderson and Sadjadpour, 2018: 10).

On the other hand, the first remarkable activity of Iranian Cyber Army is that they managed to deactivate Twitter for long hours during protests in the process of Green Activity. It is also claimed that Iranian Cyber Army arranged cyber attacks towards international press corporations with the justification that they supported opposition activities in Iran. In this frame, it is claimed that there was Iranian Cyber Army at the background of the cyber attack towards BBC Iran Service in 1st of March, 2012 (BBC, 2012).

As indicated, along with the support provided to the Iranian Cyber Army, Islamic Revolution Guards occasionally organise cyber-attacks by their own means. In this scope, some Iranian human rights activists were arrested by Islamic Revolution Guards in March 2010. Before these arrests, social media accounts and other internet use opportunities of the aforementioned activists were systemically attacked by Islamic Revolution Guards. Likewise, in December 2013, cyber-attacks were organised against nine human rights activists and independent media sites by Islamic Revolution Guards. Both attacks were accepted by Islamic Revolution Guards with an official statement (Anderson and Sadjadpour, 2018: 22).

It is claimed that Ministry of Intelligence of the Islamic Republic of Iran has remarkable capacity and potential of directly organising cyber-attacks. At this point, it is asserted that the Ministry of Intelligence organises this kind of attacks through proxy organisations. For example, obtaining approximately 1 million documents of the Kingdom of Saudi Arabia's Ministry of Foreign Affairs through cyber espionage means by an organisation called Yemen Cyber Army and disclosing these documents via Wikileaks can be evaluated within this scope (Paganini, 2015). During this revelation process, deliberate non-disclosure of documents of Iran and Russia supports this evaluation. In this respect, it can strongly be assessed that as a proxy organisation Yemen Cyber Army has a relation with Iran Ministry of Intelligence.

Basij Paramilitary Force plays an efficient role within the cyber capacity of Iran as a more amateur organisation compared to Iran Cyber Army and Cyber Security Command. The most crucial role of Basij Forces within Iran's cyber capacity is to ensure support of its members for pro-regime views in the Iran's national internet field by providing them training and technical opportunities (BBC Persian, 2018: 3).

Law Enforcement Force of the Islamic Republic of Iran established an organisation called FATA with the aim of fighting internet-based cyber-crimes in January 2011. This organisation investigates cyber-crimes and performs major duties with regards to monitoring and investigating internet cafes, social media channels and VPN opportunities where opposing groups may be organised (BBC Persian, 2018: 4).

Committee to Identify Unauthorised Sites was founded in January 2009. As can be understood, this committee operates with the aim of identifying internet sites not officially authorised by the regime. This committee was founded with the instruction of High Council of Cultural Revolution (Shorā-ye Enghelāb-e Farhangi) and it carries out its duties under the supervision of this council (BBC Persian, 2018: 5).

Within the scope of efficient activities of the aforementioned organisations, Iran becomes the embodiment of how a militarily weak country within international system can reach an effective cyber-attack capacity. As stated, there are major deficiencies within the cyber capacity of Iran, which is categorised as the third biggest cyber threat following Russia and China by USA.

Embargo imposed upon Iran in this framework hampers Iran to technologically develop a more sophisticated cyber-attack capacity (Anderson and Sadjadpour, 2018: 14). In this respect, Iran's cyber capacity cannot reach a more professional since its need for external assistance, which have been sought to be provided by states such as Russia, China and North Korea governing their foreign politics processes through anti-USA policies (Anderson, 2017). For example, it is claimed that Iran has been making huge effort to supply internet filter software especially through China's Huawei Telecom Company (Stecklow, 2012). As can be seen, some cyber-attacks claimed to be planned by Iran remain at an amateur and not sufficiently well-organised level due to these handicaps (Anderson, 2017).

Another important consequence of these handicaps is related to the fact that Iran has to choose its cyber attack targets from among institutions and organisations that relatively have lower security measures and is of lesser significance. For example, hacking of Voice of America website can be evaluated within this category (Voice of America, 2011).

At this point, if we examine the nature of cyber attacks claimed to be organised by Iran, it can be understood that Iran's cyber attack operations aim at both external and internal targets. External targets are states such as USA, Israel and Saudi Arabia that Iran has problems with regarding its foreign politics and on the other hand, internal targets are organisations opposing the regime.

5. Iran's Cyber Attack Strategy And Targets

Cyber space is a field which holds asymmetrical advantages for states that are not global powers like Iran. For example, although Iran is conventionally a far more underdeveloped power compared to USA, it does not avoid being in a cost-efficient, risk free and cover power struggle in cyber space with USA by benefiting from advantages of cyber space (IHLS, 2013).

In addition to this, cyber space is an appropriate field for use of external sources. Even though Iran itself does not have efficient cyber attack weapons or experts/hackers, it can supply these deficiencies from external sources. Anonymous structure of cyber space, that is its feature to hide the source of attack, provides advantage for Iran. In this respect, Iran does not avoid organising cyber-attacks to countries such as USA, Saudi Arabia and Israel that it has problems with in foreign policy.

Besides, by supporting organisations, like Hizbollah, being closer to itself, it strives to get these organisations have ability and capacity of organising cyber attacks within the scope of its foreign policy interests (IHLS, 2013).

Iran remarkably invests in its cyber attack capacity following the Stuxnet Attack. One of the most important reasons of this strategy is to constitute deterrence against cyber attacks that may similarly be organised by USA, Israel or other enemy states in the future. Besides, having a cyber attack capacity against any conventional attacks that might be organised in the future supports Iran's military deterrence in the Middle East (IHLS, 2013).

Upon 2010, investments of Iran on its cyber attack capacity have continuously increased. In this scope, this budget having been claimed to be $ 76 million in 2011 is asserted to reach approximately $ 1 billion by the end of 2013 (Wheeler, 2013). On the other hand, it is argued that Islamic Revolution Guards holding a major part of Iran economy have employed approximately 120.000 civilians with the aim of including them in Iran's cyber defense capacity (Zakariaa, 2014).

Within the scope of the indicated advantages, Iran does not abstain from organising cyber attacks against states it has accepted as enemies within the international system by utilising opportunities and capabilities provided by cyber space. And yet, these attacks are generally in the forms of DDoSs (Distributed Denial of Service Attack), web site hacking attacks, cyber espionage activities, etc.

In this context, in September 2012, DDoS attacks were organised against USA finance sector by a group claimed to be supported by Iran and called Izz ad-Din al-Qassam Cyber Fighters. During these cyber attacks named Babel Operation, USA's banking systems were battered by DDoS attacks. According to data of Federal Bureau of Investigation (FBI), these attacks were conducted with a speed of 140 gigabits/second (U.S. National Security Agency, 2015). During these attacks, 46 major finance companies and banks such as JP Morgan Chase (JPM.N), Wells Fargo (WFC.N) and American Express (AXP.N) were affected (Reuters, 2016). These attacks have continued in the following years and yet they were not as effective as the first attacks organised in July 2013. During these cyber attacks, many banking transactions could not be performed, account-holders could not withdraw money from their accounts, and internet banking came to a halt. It was claimed that the loss was about ten millions of dollars. The Babel Operation was recorded as the most efficient cyber attack claimed to be organised by Iran against USA (U.S. National Security Agency, 2015).

Another important cyber attack claimed to be supported by Iran against USA is the attack organised against intranet system of Navy Marine Corps in August 2013. During these attacks, some confidential information and documents of Navy Marine Corps were stolen within the scope of cyber espionage operation (The Wall Street Journal, 2013).

It is asserted that Iran organises cyber attacks in various terms to Israeli targets. In this framework, DDoS attacks were organised against Israel Defense Forces during the summer months of 2014. However, these attacks were prevented by Israel's powerful defense infrastructure. Furthermore, internet infrastructure of American Israel Public Affairs Committee (APIAC) was hacked by cyber attacks in 2014 (International Business Times, 2014).

As in the example of APIAC, cyber attacks of Iran targeting against Israel can be successful in lower-profile targets. The most important reason of this is the powerful cyber defense infrastructure of Israel. In this context, Israel can easily prevent many attacks claimed to be organised by Iran thanks to its powerful cyber defense system (Anderson and Sadjadpour, 2018: 35).

The most important target of Iran's cyber attacks is Saudi Arabia, with whom it has a power struggle in the Middle East, against whom it wages proxy war through its proxies in Yemen, Syria and Iraq, and with whom it goes through a tension for Lebanon and Bahrain. In this context, critical infrastructure of Saudi Arabia's Saudi Aramco Company was severely damaged by cyber attacks

claimed to be supported by Iran between 15 and 22 August 2012. It was asserted that both companies lost hundreds of millions of dollars during these attacks (For detailed information, see Anderson and Sadjadpour, 2018: 33-34).

In these attacks, Saudi Aramco Petroleum Company's 30.000 Windows operating system based computers were hacked by erasing all critical documents, e-mails and information on these computers by a malicious software called Shamoon and adding a burning US-flag to these computers (Siber Bülten, 2015).

It is claimed that the real aim of these attacks was to halt petroleum and gas flow at national and international level. Even though these attacks caused serious damage, they were not successful. Shamoon virus was written in a way to irreversibly erase data on hard discs of infected computers. Therefore, in spite of the fact that the virus affected the company's production and distribution capacity, the company was severely damaged by the deletion of production and distribution data (Siber Bülten, 2015).

The attack was undertaken by a hacker group called Cutting Sword of Justice. At the investigation stage of this attack, it was identified that the attack was organised in various countries from four different continents. Taking into consideration that Saudi Arabia sent military corps to Bahrain and supported groups opposing the Assad regime in Syria during the period of these attacks, it was asserted that Tahran government was the driving force behind these attacks. Religious symbols such as selection of Laylat Al-Qadr, a sacred day for Muslims, for the attack and calling the undertaking hacker group "Cutting Sword of Justice, which is the attributed name of Prophet Ali in Shia belief, fuelled the suspicion that Iran was behind the attack (Siber Bülten, 2014).

It is suggested that Afghanistan was among states targeted by cyber attack and espionage activities of Iran. In this scope, within the context of cyber attack and espionage capacity it has developed after 2010, it is expressed that Iran occasionally organised espionage activities against Afghanistan National Radio, Ministry of Education and other institutions (Anderson and Sadjadpour, 2018: 14).

It was claimed by the Observer on 22 April 2015 that power cuts in Turkey dated 31 March 2015, which lasted for 12 hours and affected more than 40 million people in 44 of 81 provinces, including Ankara and Istanbul, were a cyber attack supported by Iran. In this context, according Micah Halpern's news titled "Iran Flexes Its Powers by Transporting Turkey to the Stone Age", shortly, he asserted that "Power outage happened on the given date was a punishment for statements of the President Recep Tayyip Erdoğan criticising Iran's policies over Yemen and therefore Turkish citizens were left without power" (Observer 2015).

In this scope, it should be noted that Jewish Micah D. Halpern is an academician specialised in the Middle East and Muslim Fundamentalism and on that date he was also working as a consultant to the USA's President on cyber attacks (Nebil, 2015). Journalist Ruhallah Zam'dan, an Iranian regime dissident, made statements on this matter to the Observer confirming this situation. First official statement on this matter indicated that power outages were caused by synchronisation inconsistency. According to the official statement made by Ministry of Energy one and a half month after the incident, it was expressed that no cyber attack was organised against power distribution system (Nebil, 2017). On the other hand, some independent electrical engineers evaluated that in that given period, it was less likely to speak of such a long-lasting and common power outage due to synchronisation inconsistency in Turkey having an interconnected electric power distribution network (Nebil, 2017).

At this point, whether these outages occurred as a result of an Iran supported cyber attack cannot be clearly confirmed or denied since there are still no official data and results. Besides, since claims

were asserted by dissident groups of Iranian regime, information on this matter cannot go beyond speculation.

In terms of displaying Iran's cyber espionage capacity, case of Iranian hacker Nima Golestaneh is remarkable. It was claimed that in connection with Iranian intelligence agencies between April 2012 and May 2013, he stole secret technologies of USA Defense Company named Arrow Tech Associates within the scope of a cyber espionage operation. Later on, this person was arrested in Turkey and extradited to USA in February 2015 (USA Today, 2015). Iran also utilises proxy organisations it directly or indirectly supports within the scope of cyber attack activities. In this context, cyber espionage software targeting Israel's defense sectors in 2012 by Hizbollah, which is claimed to be supported by Iran for having efficient cyber attack capacity, was detected by an Israeli cyber security company called CheckPoint before it was activated (Caravelli and Maier, 2016: 25).

Similarly, in April 2013, Twitter account of Associated Press was hacked by a proxy group called Syrian Electronic Army, which was claimed to have an active cyber attack capacity with the support of Iran, and due to speculative posts shared through this account, a decrease worth $ 130 million occurred in New York Stock Exchange (For detailed information, see Caravelli and Maier, 2016: 25). As is seen, external targets of Iran's cyber attack operations are generally countries, such as USA, Israel and Saudi Arabia, it is in competition and conflict with in international system. Besides, it can be understood that Iran does not refrain from planning covert activities within the scope of cyber espionage operations.

On the other hand, internal targets of Iran's cyber operations are basically dissidents of the regime. These targets are state officials, reformist politicians, media employees, local religious leaders, religious minorities, cultural figures and terror organisations opposing the regime, various groups and separatist movements (Anderson and Sadjadpour, 2018: 40). Although Iran's systematic of politics is holistically displayed to the outer World, existence of different factions and fierce competition among these factions is known. In this context, it is suggested that cyber capacity of Iran Intelligence Ministry and Islamic Revolution Guards is an instrument used in the struggle between these factions. In this respect, during the political struggle between Iran's President Hassan Rouhani and the previous President Mahmoud Ahmadinejad, their relatives and bureaucrats and business people in the immediate circle were claimed to be the target of these cyber espionage operations (IranWire, 2013).

It was speculated in Iranian society that politicians such as the previous President Mohammad Khatami who advocated reformist policies in Iran, previous presidential candidates Mehdi Karroubi, Mir, Hossein Mousavi, previous Deputy Minister of Culture Mohammad Ali Abtahi and their immediate circle were exposed to cyber espionage and social engineering activities of Iran's Intelligence Ministry and Islamic Revolution Guards (IranWire, 2013). Case of Jason Rezaian working as Iran Representative of Washington Post is crucial in terms of his being a target of cyber activities of Islamic Revolution Guards. In this context, e-mail accounts of Jason Rezaian were hacked by Islamic Revolution Guards. And this was used as the basis of indictments about e-mail communications (Washington Post, 2016).

Iran's heterogenic social structure causes Iran to regard different ethnic and religious groups as target to be continuously kept under control for the purpose of the regime's security and survivability. In this context, communities with Bahai belief frequently become the targets of cyber espionage operations of Iran's Intelligence Ministry and Islamic Revolution Guards. A great majority of people with Bahai belief live in several states of USA and Haifa in Israel due to oppressions in Iran. Therefore, people with Bahai belief living in this city and states are targets of Iran's cyber espionage operations. In this respect, in April 2014, it was revealed that e-mail communication system of USA's Bahai Organisation was hacked by a cyber attack supported by Iran (Anderson and Sadjadpour, 2018: 44).

Iran regime powers can frequently apply to cyber espionage operations disclosing deficiencies of leading people acting as cultural figures due to the reason that they undermine the social structure.

By doing so, they aim at ensuring legitimacy of the regime by discrediting individuals with a different life style compared to cultural standards determined by the regime. In this framework, some models who gained popularity in social media were arrested and their social media correspondences and pictures were disclosed in January 2016. This disclosure activity was performed by Islamic Revolution Guards within the scope of social media and internet monitoring activity called Spider Operation (The Telegraph, 2016).

As indicated, terror organisations opposing the regime, various groups and dissident movements are among internal targets of Iran's cyber operations. In this scope, in 2015, Simay Azadi Television, broadcasting in USA as a dissident of Iran's regime, and social media accounts and internet infrastructure of Iran-America Society in Texas were exposed to advanced cyber attacks supported by Iran (CNRI, 2015). Besides, internet infrastructure of the Jundullah Organisation supported by some Sunni groups in Sistan and Baluchestan states of Iran was asserted to be hacked by a cyber attack supported by Iran in July 2010 (Anderson and Sadjadpour, 2018: 47). Similarly, internet infrastructure of Newroz TV related with Kurdistan Free Life Party (Partiya Jiyana Azad / PJAK) and Kurdistan Workers' Party (Partiya Karkerên Kurdistanê / PKK) was hacked by cyber attacks supported by Iran in 2014 and 2015 (Anderson and Sadjadpour, 2018: 47).

It is stated that civil society organisations opposing the regime are also faced with cyber operations claimed to be supported by Iran. In this scope, Eurasian Foundation operating in Washington DC by the support of USA plans various social development projects for countries in the previous Soviet Union geography as well as Iran. It is claimed in an article featured in an Iran-based newspaper called Kayhan in February 2014 that the aforementioned foundation and its activities was the centre of espionage activities against Iran. Following this news, internet infrastructure of the aforementioned foundation was exposed to cyber attacks lasting for 2 years and claimed to be supported by Iran (Anderson and Sadjadpour, 2018; 48).

6. Conclusion

Iran's cyber attack strategy development planning took shape upon 2010 Stuxnet Attack targeting its nuclear facilities and claimed to be planned by USA and Israel. Iran's efforts to develop its cyber attack capacity have played a major role in turning Iran to a crucial actor in cyber space thanks to measures taken in the following periods.

In this context, Iran targets at having a powerful cyber attack capacity. Main reason behind this target underlies its intention to benefit from asymmetrical advantages provided by cyber space in the Middle East. In this respect, although Iran is conventionally a far weaker power than USA, it does not avoid struggling with USA in cyber space by benefiting from advantages of cyber space.

Another reason why Iran wants to increase its cyber attack capacity is its wish to constitute deterrence against cyber attacks to be organised by USA, Israel or other hostile countries. Besides it is obvious that having an efficient cyber attack capacity will provide Iran military deterrence against any conventional attack likely to be organised against Iran in the upcoming period.

High Council of Cyber Security, Islamic Revolution Guards, Iran Intelligence Ministry and Cyber Security Command, which determine cyber policies, and Iran Cyber Army, which is a proxy organisation in connection with these institutions, play an important role with regards to cyber attack capacity. By taking advantage of anonymous nature of cyber space, Iran supports groups organised as proxy structures not only domestically but also internationally. In this respect, Hizbollah, which is claimed to be in connection with Iran government, Yemen Cyber Army and Syria Electronic Army play an important role in Iran's cyber attack capacity (See more at; Pierluigi, 2015)

Within the scope of efficient activities of the aforementioned organisations, Iran is the embodiment of how a militarily weak country within international system can reach an effective cyber-

attack capacity. There are important advantages of Iran's being at a lower point of technology development and its use with regards to cyber defense capacity. The fact that a major part of Iran's critical infrastructure is still being controlled by mechanical technologies provides a natural advantage for Iran in terms of cyber defense. Thus Iran weighs more importance to efforts of monitoring internet and social media, the main medium where anti-regime movements are organised, rather than primarily preferring to protect its critical infrastructures in its cyber defense strategy from cyber attacks.

On the other hand, cyber attacks to be claimed to be organised by Iran have internal and external targets. External targets are mainly countries Iran has problems with in foreign politics such as USA, Israel and Saudi Arabia. Whereas it is observed that internal targets are comprised of structures opposing the regime. These internal targets are state officials, reformist politicians, media employees, local religious leaders, religious minorities, cultural figures and terror organisations opposing the regime, various groups and separatist movements that display a faction tendency within the regime.

On the other hand, Iran's internal and external defence priorities basically include protecting integrity and political independence of the regime and the country having a heterogeneous social structure, protecting and developing Iran society and Shia heritage and legacy in the Middle East, ensuring regional power role, gaining advantage against states and groups perceived as regional threat, enhancing its efficiency in regional leadership struggle, its will to struggle external interventions targeting the country's integrity and political independence. Within this scope, it can also be seen that Iran's cyber attack targets are determined in accordance with Iran's internal and external defense priorities.

As a conclusion, it can be observed that in terms of defense and attack, Iran's cyber capacity has started to rapidly develop with investments made after 2010. However, embargo imposed upon Iran prevents Iran to technologically develop a more sophisticated cyber-attack capacity. Besides, Iran's cyber capacity needs external assistance and therefore its efficiency cannot be elevated to a more professional level. In this scope, it can be envisaged that if Iran does not face any problems regarding supply and development of external technology due to embargo practices, it can further develop efficiency of its cyber security strategy by adding further to current infrastructure in the future. How this embargo will continue, under which conditions it will be determined, whether Iran will break this embargo process, to what extent Russia, China and North Korea, with whom Iran has serious relationship with regards to Iran's technology transfer, will be determinant in development of Iran's cyber attack capacity.

If Iran tackles its problems regarding embargo, it is likely that as a solution Iran can more frequently apply to the alternative of benefiting from cyber space technologies' appropriate structure of use of external assistance. In this respect, in the future Iran will more easily be able to supply various cyber attack applications from cyber space by paying their fees with opportunities to be provided by cyber space, and to employ paid hackers and cyber experts. However, this alternative should also be known to a limited solution.

As it is seen, within the scope of embargo related handicaps regarding technology development, cyber attacks to be planned by Iran will remain at an amateur and not well-organised level. Due to these deficiencies, it is likely that targets of Iran's cyber attack to be organised in the future will be from among institutions and organisations that relatively have lower security measures and is of lesser significance. It can also be expressed that Iran will make every effort to develop its cyber attack capabilities and opportunities through proxy organisations by supporting cyber capacity of groups close to itself such as Yemen Cyber Army, Syria Electronic Army and Hizbollah. Iran already strives to efficiently benefit from proxy organisations in its current cyber attack strategy. In this respect, it is likely that Iran will further develop its proxy cyber attack systematic through new investments to be made by itself.

It can be indicated that one of the most important handicaps that hampers Iran to develop an efficient cyber capacity is brain drain from Iran to Western countries, which occurs in the quest of a better life opportunity. In this context, it is estimated that approximately 150.000 skilled labours emigrate from Iran every year and the cost of this immigration for Iran is around $ 150 billion (MEHR News Agency, 2014). In this respect, if Iran government does not succeed to keep the aforementioned skilled labour in the country, it is clear that it will face severe problems with constituting an efficient cyber security capacity.

REFERENCES

American Foreign Policy Council, (2013); *The Iranian Cyber Threat, Revisited*, https://china.usc.edu/sites/default/files/legacy/AppImages/house-2013-berman-cyber-threats.pdf, (Erişim Tarihi: 29.11.2018)

Anderson, C. ve Sadjadpour, K. (2018); *Iran's Cyber Threat*, Report published by Carnegie Endowment for International Peace.

Anderson, Collin. (2017); *Bears and Kittens, and Startup Cybersecurity Companies*, https://medium.com/@collina/bears-and-kittens-and-startup-cybersecurity-companies-5c8e037ea75c, (Erişim Tarihi: 01.07.2018).

Ateş, S.S. vd. (2017); Investigating Critical Points of Cyber Security: Prevention Terror Attacks in Airports, Turkish Studies, 12(32), ss. 33-48.

BBC, (2012*); Cyber-attack on BBC leads to suspicion of Iran's involvement*, https://www.bbc.com/news/technology-17365416, (Erişim Tarihi:30.12.2018).

BBC, (2016); *Iran rolls out domestic internet*, https://www.bbc.com/news/technology-37212456, (Erişim Tarihi:01.07.2018)

BBC Persian, (2018); *Structure of Iran's Cyber Warfare*, http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf, (Erişim Tarihi: 01.02.2019).

Caravelli, J. ve Maier, S. (2016); *Deciphering Iran's Cyber Activities*, a report published by King Faisal Center for Research and Islamic Studies.

CNN, (2017); *UN experts urge Iran to respect rights of protesters, end Internet crackdown*, https://edition.cnn.com/2018/01/05/middleeast/iran-protests-united-nations-intl/index.html, (Erişim Tarihi:01.01.2019).

CNRI, (2015); *Mullahs Resort To Cyber Terrorism*, https://www.ncr-iran.org/it/index.php/comunicati-stampa/resistenza-iraniana/208-mullahs-resort-to-cyber-terrorism, (Erişim Tarihi:30.06.2018).

Darıcılı, A. B. (2017); *Siber Uzay ve Siber Güvenlik; ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi*, Dora Yayıncılık, Bursa / Türkiye.

Darıcılı, A. B. ve Özdal, B. (2017); *Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi*, Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi (BİLİG), Avrasya'nın Siyasal İktisadı Özel Sayısı, ss. 121-146.

Efegil, E. (2012); *İran'ın Dış Politika Yapım Sürecini Etkileyen Unsurlar*, Ortadoğu Analiz, 4 (48), ss. 53-68.

IHLS, (2013); *Iran on the Cyber Offensive*,http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Iran%20on%20the%20cyber%20offensive.pdf, (26.06.2018).

International Business Times, (2014); *Anonymous to Attack AIPAC in Crusade Against Israel*, https://www.ibtimes.co.uk/anonymous-attack-aipac-israel-cyber-crusade-308994, (Erişim Tarihi:01.02.2019).

Iran's News Update, (2014); *Layers of Internet Censorship in Iran*https://irannewsupdate.com/news/infightings/1115-layers-of-internet-censorship-in-iran.html, (Erişim Tarihi: 26.12.2018).

IranWire (2013); *Zarif, Hacked But Unscathed*, https://iranwire.com/en/features/117, (Erişim Tarihi: 15.11.2018).

Kamacı, Y. (2013); *2009'dan 2013'e Yeşil Hareket'in Yolculuğu*, http://politikaakademisi.org/2013/07/01/2009dan-2013e-yesil-hareketin-yolculugu/, (Erişim Tarihi: 26.12.2018).

MEHR Agency, (2014); *Iran Loses $150 Billion a Year Due to Brain Drain*, http://en.mehrnews.com/news/101558/Iran-loses-150-billion-a-year-due-to-brain-drain, (Erişim Tarihi: 26.06.2018).

Nebil, F. S. (2015); *Observer yazdı: Elektrik kesintisi siber saldırıydı!*, http://t24.com.tr/yazarlar/fusun-sarp-nebil/ingiliz-observer-yazdi-elektrik-kesintisi-siber-saldiriydi,11760, (Erişim Tarihi: 08.02.2019).

Nebil, F. S. (2017); *İranlı Gazeteci Açıkladı: Elektrik Kesintisi Siber Saldırıymış*, http://turk-internet.com/portal/yazigoster.php?yaziid=56620, (Erişim Tarihi: 08.02.2019).

Observer, (2015); *Iran Flexes Its Power by Transporting Turkey to the Stone Age*, http://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/, (Erişim Tarihi: 08.02.2019).

Pierluigi P. (2015); *Yemen Cyber Army will release 1M of records per week to stop Saudi Attacks*, https://securityaffairs.co/wordpress/37357/hacking/yemen-cyber-army-1m-saudi-records.html, (Erişim Tarihi: 09.02.2019).

Reuters, (2016); *U.S. indicts Iranians for hacking dozens of banks*, *New York dam*, (Erişim Tarihi: 10.02.2019).

Reuters, (2015); *Iran's elite Revolutionary Guards are ramping up domestic surveillance*, http://www.businessinsider.com/r-irans-guards-increase-monitoring-of-social-media-state-tv-2015-3, (Erişim Tarihi: 07.02.2019).

Sanger, D. (2011); *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0, (Erişim Tarihi:02.12.2018).

Siber Bülten, (2014); *ARAMCO Saldırısı*, https://siberbulten.com/siber-saldirilar-2/aramco-saldirisi/, (Erişim Tarihi: 30.11.2018).

Slavin, B. and Healey, J. (2013); *Iran: How a Third Tier Cyber Power Can Still Threaten the United States*, Issue Brief published by Brent Scowcroft Center on Interntional Sucurity South Asia Center.

Small Media, (2018); *Internet Censorship in Iran*, https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded_Ch2_InternetCensorship.pdf, (Erişim Tarihi: 30.11.2018).

Stecklow, S. (2012); *Exclusive: Huawei partner offered U.S. tech to Iran*, https://www.reuters.com/article/us-huawei-iran/exclusive-huawei-partner-offered-u-s-tech-to-iran-idUSBRE89O0E520121025, (Erişim Tarihi:03.02.2019).

The Department of Defence of the USA (2015); *The DOD Cyber Strategy*, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, (Erişim Tarihi: 26.06.2018).

The Wall Street Journal, (2013); *U.S. Says Iran Hacked Navy Computers*, https://www.wsj.com/articles/us-says-iran-hacked-navy-computers-1380314771, (Erişim Tarihi: 01.12.2018).

The Telegraph, (2016); *Iranian models arrested and forced to give public self-criticism for posting pictures without headscarves*, https://www.telegraph.co.uk/news/2016/05/16/iranian-models-arrested-for-posting-pictures-without-headscarves/, (Erişim Tarihi: 26.06.2018).

USA Today, (2015); *Feds: Iranian hacker targeted Vermont aerodynamics firm*, https://www.usatoday.com/story/news/nation/2015/07/29/feds-iranian-hacker-targeted-vermont-aerodynamics-firm/30860681/, (Erişim Tarihi, 01.12.2018).

U.S. National Security Agency; (2015); *Iran - Current Topics, Interaction With GCHQ*, https://theintercept.com/document/2015/02/10/iran-current-topics-interaction-gchq/, (Erişim Tarihi: 01.12.2018).

Voice of America, (2011); *Iranian Hackers Attack VOA Internet Sites* https://www.voanews.com/a/iranian-hackers-attack-voa-internet-sites-116678844/172741.html, (Erişim Tarihi: 01.12.2018).

Washington Post, (2016); *10 harrowing details about Jason Rezaian and Yeganeh Salehi's imprisonment in Iran*https://www.washingtonpost.com/news/worldviews/wp/2016/10/03/10-harrowing-details-about-jason-and-yeganeh-rezaians-imprisonment-in-iran/?utm_term=.22348bfd95ad, (Erişim Tarihi: 01.12.2018).

Wheeler, A. (2013); *Iranian Cyber Army, The Offensive Arm of Iran's Cyber Force*, *www.phoenixts.com/blog/iranian-cyber-army*, (Erişim Tarihi: 03.01.2019).

Zakariaa, F. (2014); *Iran's Emergence as a Cyber Power*,http://www.strategicstudiesinstitute.army.mil/index.cfm/articles/Irans-emergence-as-cyber-power/2014/08/20, (Erişim Tarihi: 10.01.2018)