ANALYSIS OF MANIPULATION OF THE RUSSIAN FEDERATION IN THE 2016 PRESIDENTIAL ELECTIONS OF THE UNITED STATES OF AMERICA WITHIN THE SCOPE OF INTELLIGENCE TECHNIQUES

Ali Burak DARICILI*

Abstract

In this study, the manipulations of the Russian Federation (RF) in the presidential election process held in the United States of America (the US) in 2016 November are examined within the scope of RF's cyber espionage and US' counter-espionage capacities. RF has managed to manipulate the election process with the cyber espionage capabilities of the military intelligence service GRU (Glavnoye Razvedyvatel'noye Upravleniye/Main Intelligence Directorate), which has become increasingly sophisticated in recent years. FBI (Federal Bureau of Investigation), which is the USA's counter/espionage capacity and the main intelligence service establishing this capacity, could not uncover this intervention process and within this framework failed to resist against the intelligence activities of a hostile country aimed at its own country. The manipulation of GRU in the US presidential elections has been constantly brought into question by the opponents of Donald Trump in order to create political oppression against him following his election as the President of the US. In this context, the intelligence activities of GRU have been revealed in detail by the relevant official intelligence services of the US. The analysis of these details has become important in terms of understanding the weaknesses in the counter-espionage system of the US coordinated under the leadership of the FBI, as well as the RF's cyber espionage capabilities dominated by the GRU.

Keywords: *RF, The US, Presidential Elections, GRU, FBI*

RUSYA FEDERASYONU'NUN AMERİKA BİRLEŞİK DEVLETLERİ 2016 BAŞKANLIK SEÇİMLERİNE YÖNELİK MANİPÜLASYONUNUN İSTİHBARAT TEKNİKLERİ KAPSAMINDA ANALİZİ

Öz

Bu çalışmada, Rusya Federasyonu (RF)'nun Amerika Birleşik Devletleri (ABD)'nde 2016 Kasım ayında yapılan başkanlık seçim sürecine yönelik manipülasyonları, RF'nin siber espiyonaj, ABD'nin ise kontr/espiyonaj kapasiteleri kapsamında incelenmektedir. RF, söz konusu seçim sürecine askerî istihbarat servisi olan GRU (Glavnoye Razvedyvatel'noye Upravleniye / Ana Askerî İstihbarat Servisi)'nun son yıllarda giderek sofistike hale gelen siber espiyonaj imkân ve kabiliyetleri dâhilinde manipüle etmeyi bir ölçüde de olsa başarmıştır. Bu müdahale sürecini ABD kontr/espiyonaj kapasitesi ve bu kapasiteyi oluşturan temel istihbarat servisi olan FBI (Federal Bureau of Investigation / Federal Araştırma Bürosu) zamanında deşifre edememiş ve bu çerçevede hasım bir devletin ülkesine yönelik istihbari faaliyetine karşı koymada başarısız olmuştur. GRU'nun ABD Başkanlık seçimlerine yönelik manipülasyonları Donald Trump'ın ABD Başkanı olması akabinde ise anılanı siyasi açıdan baskı altına almak amacıyla Trump'a muhalif çevrelerce sürekli olarak gündemde tutulmaya başlanmıştır. Bu kapsamda da GRU'nun söz konusu istihbari faaliyetleri ABD'nin ilgili resmî istihbarat yapılanmaları tarafından detaylarıyla ortaya konulmuştur. Bu detayların analizi ise ABD'nin FBI önderliğinde koordine edilen kontr/espiyonaj sistematiğindeki zafiyetlerin anlaşılmasının yanı sıra RF'nin GRU tarafından domine edilen siber espiyonaj kabiliyetlerini ortaya koymak bakımından önemli hale gelmiştir.

Anahtar Kelimeler: *RF, ABD, Başkanlık Seçimleri, GRU, FBI*

* Dr. Faculty Member, Bursa Technical University, Faculty of Humanities and Social Sciences, Department of International Relations, Bursa / Turkey, E-mail: ali.daricili@btu.edu.tr, https://orcid.org/0000-0002-3499-1645.

Makale Geliş Tarihi: 26.10.2018 Makale Kabul Tarihi: 07.03.2019

INTRODUCTION

The foundations of competition between the RF and the US today are based on the competition between the KGB (the Comitet Gosudarst Bezopasbosti / Committee for State Security) and the CIA (Central Intelligence Service) during the Cold War. The Soviet Union and the US, which have been struggling in the fields of military and technology as well as intelligence activities in the Cold War period, have laid the foundations of the internet technologies that form the so-called cyber space today with the planning they introduced in this period.

The US founded ARPA (Advanced Research Projects Agency) in February 1958 to compete with the Soviet Union in the scientific field during the Cold War period. The content of the projects in ARPA were designed to cover ballistic missile defense as well as space research (Bıçakçı, 2014: 103). This project was the beginning of internet technologies along with the development of a planning that could enable scientists working within ARPA to operate within a single communication systematic based on network technologies. ARPA project, together with this communication system, is named as ARPANET (Darıcılı, 2017a: 4).

The necessity to develop various measures in order to prevent ARPANET from being affected by the attacks in the event of a possible nuclear war with the Cuban Crisis is better understood. With studies in this direction, it was ensured to create a network structure where communication could be maintained with the largest group which could remain functional after the nuclear attack by providing electrical connection. Thus, the interconnected ARPANET components are first connected with the commercial network in the National Physical Laboratory in the UK and the Cyclades which is a research network in France. Thus, the first core infrastructure of the Internet with global dimension was created (Bıçakçı, 2013: 6).

In response to these steps taken by the US, KGB has begun to develop some countermeasures. KGB established new and strong institutional structures In this context, when the space competition accelerated as well as the military competition in the between the two blocks was in progress in the 1960s, significant part of the KGB's foreign operations focused on procuring the technologies developed in the US through espionage methods (Darıcılı, 2017b: 139). With the 1980s, the Soviet Union brought forward a very important planning which has theoretical and practical impacts on the current development of cyber space technologies with the proposal of RMA (Revolution in Military Affairs) designed by Marshal Nikolai Ogarkov (See at more; Mowthorpe, 2015: 137-153).

The main objective of this new approach, which was put forward by Ogarkov, was to make the Soviet Army, which had been more cumbersome in nature than the US armed force, equipped with a more effective structure that is reinforced and managed by network technologies. This project of Ogarkov has never been realized because of the competition between the elements that constitute the Politburo (Politicheskoye Byuro) of the period. The US side has planned to respond to the RMA approach, which was put forward by Ogarkov, with the Star Wars Project (Strategic Defense Initiative). "Strategic Defense Initiative" announced to the public with the speech of Ronald Reagan in 1983 was planned as a project aiming at destruction of enemy missiles by means of space-based equipment. (Başbaşoğlu, 2011: 75) Although this project has never been realized like RMA, it is important that it is the first concrete planning in terms of the possibility of use of internet technologies for reforming the classical conventional power structures of the armed forces. With these intellectual developments, which started to develop in the 1980s, states, that started to become aware of the successful results of the commercialization of the internet since the 1990s, began to see the potential provided by cyber space as a new opportunity to develop their military capabilities.

As summarized above, the competition between the US and the Soviet Union in the military and technology spheres during the Cold War period has evolved into a new dimension today along with the claims that the presidential election processes in the US in November 2016 were manipulated by the GRU. These claims can be stated in the most basic form as that the e-mails of some politicians and consultants which are active within the body of DNC (Democratic National Committee) particularly Hillary Clinton's have been procured by the RF through cyber-attack methods and that some of these e-mails are leaked to the press and thus the US election process have been manipulated in favour of the other presidential candidate Donald Trump in accordance with the national interests of the RF. On the other hand, the mentioned claims were constantly brought into question by the opponent parties after Trump has won the presidential elections. In this context, official intelligence and security organizations of the US have prepared various reports revealing the processes in question with details.

1. CLAIMS THAT RF MANIPULATED THE US PRESIDENTIAL ELECTIONS IN THE OFFICIAL DISTRICTS

Global powers' involvement in election manipulations and their interventions in the internal affairs of states are frequently seen cases in the history of international relations. In this context, it has been claimed that the United States has sabotaged the electoral processes many times in Latin American countries in order to intervene politically since the beginning of the 20th century (See more at; Parag, 2008). These interventions in the elections are generally preferred because they are a less costly

method and they often include elements such as bribery, assistance to political parties, destabilization campaigns and media manipulations (Williams, 2012: 40).

At this point, several examples can be mentioned about the intervention of the US in the electoral processes. For example, the US which helped assassination Rafael Trujillo in 1961 in the Dominican Republic, provided budget and propaganda support for the victory of Juan Bosch in the presidential elections (See at more; Skidmore and Smith, 2005: 422-423). Eduardo Montealegre was supported in Nicaragua, another Latin America country, for his victory in the elections in 2006 and any kind of media, budget and campaign support was provided to unite the voters voting for the liberal parties under a single candidate (Keskin, 2016: 81).

In addition, the effort of the US to shape the political system in Afghanistan, which it considers as a buffer country between itself and the RF, was reflected in the presidential elections in 2009. Robert Gates, the US Secretary of Defense at that time, clearly admitted in an interview that the US manipulated the 2009 Afghan elections. Gates stated that "*the elections were postponed in defiance of the constitution and efforts were made in order to prevent re-election of the President of the period Hamid Karzai"*. It is revealed that a great number of "suspicious" cases occurred in the presidential elections held under the shadow of the United States in 2014 and the discussions regarding the results of the elections kept for months. Similarly, one of the countries which the US intervened in the elections and political order under the motto of "*fighting communism*" was Italy in the heart of Europe. The CIA, which provided millions of dollars of support to their collaborators in Italy for election of the Christian Democracy instead of the Communist Party in the elections held in 1948, has determined the faith of the elections in this country by this means. In this process, the CIA played an active role and transferred millions of US Dollars to the Christian Democracy for campaign support (See more at; Pero, 2001).

Nowadays, social media opportunities with the technological changes in the field of information have caused significant changes in the manipulation and provocation activities that the secret services such as GRU tried to carry out with the classical techniques. Social media has begun to be accepted as a convenient medium by secret services in the planning and development of such activities. The reason of this preference is that the manipulation activities carried out on social media shall be assessed within the framework that they are interesting, more understandable and cheaper, have a flexible structure according to the needs and can be revised continuously, can be directed to the target group easily, rapidly and simultaneously and in a very short time, provide opportunities of a structure without geographical boundaries and that the cryptographic software characteristics of the social media applications enable the users to hide their identity easily (See more at; NATO Strategic Communications Centre of Excellence, 2016).

In this context, It was brought forward that Russian Intelligence Services (RIS) was engaged in manipulation activities for the 2016 Presidential elections for the first time by the DNC. Later, these claims were tried to be elaborated by the reports prepared by the FBI, CIA, DHS (The Department of Homeland Security) and NSA (National Security Agency). Finally, an indictment was filed regarding the mentioned claims by the Washington DC District Court (The US District Court for The District of Columbia) on July 13, 2018 as a result of the investigation carried out by the Specially Authorized Prosecutor Robert Mueller and 12 GRU members were accused directly in this indictment (See more at; The Department of Justice, 2018).

On the other hand, prior to the indictment in question, RF was openly charged as the planner of these cyber-attacks in a report jointly prepared by the FBI and DHS regarding these cyber-attacks. In addition, it was brought forward in the media statement published with the report in question on December 29, 2016 that Russian intelligence elements were planning cyber-attacks targeting the US government agencies, non-governmental organizations, universities, US critical infrastructures, think tanks, technology producing companies beyond the cyber-attacks noticed in the mentioned report (Department of Homeland Security, 2016a).

Furthermore, it has been mentioned in another media statement made on December 30, 2016 by the DHS that civil and military intelligence structures of the RF carried out sophisticated and aggressive operations targeting the US government and the citizens in recent periods, the RF launched cyber espionage operations through target oriented and phishing methods, which are called as "spread phishing", against the government institutions, universities, civil society and think tank organizations, political parties and revealed the procured confidential information to the public through third partners and several technical details regarding software and application procedures of the mentioned "spread phishing" operations were shared with the public (See at more; Department of Homeland Security, 2016b)

Moreover, it has been stated in a joint report on the subject by the FBI, CIA and the NSA on 7 January 2017 that Putin gave the order to manipulate the US Presidential election process in 2016, that the main purpose of this manipulation was to undermine the public confidence in the Democratic Party, that the Democratic Party candidate Clinton clearly suffered damage and that the other presidential candidate Donald Trump also benefited from this case (See at more; Office of the Director of National Intelligence, 2017).

In the aftermath of the open accusations made by the US government agencies to the RF government, it was decided that 35 Russian diplomats, who were claimed as members of the GRU by the Barack Obama administration of the period, are deported on charges of working in the cyber-attacks targeting the US presidential

elections and that the Russian diplomatic missions in Maryland and New York are closed (Sputniknews Portal: December 12, 2016)

In the face of the deportation decision, the RF party stated that it does not accept the charges. It was expressed in the statement made by Putin regarding the subject that "*the developments are considered as new hostile steps taken by Washington government and as provocation, that they will not depart anyone and they will determine the response against the US according to the attitude of the Trump administration."* (Sputniknews Portal: December 30, 2016). On the other hand, the "*Patriotic Russian Hackers"* statement made by Putin on June 1, 2017 in the context of the issue has found a wide resonance in the world public opinion. In response to a question regarding Democratic Party Hack Scandal Putin state that; "*RF has never involved in such a thing, perhaps patriotic Russian hackers may have organized a cyber-attack, and that if hackers are patriotic, they can begin to make their own contributions to waging a good war against those casting aspersions on Russia, that this is possible theoretically and they did not involve in any hacking operations at state level and they are not planning to involve*." (CNN International: June 2, 2017).

The details of the reports put forward by the US official security and intelligence agencies regarding these allegations are included in the indictment prepared after the Muller Investigation. It is claimed with details and documents in this indictment (See more at; The Department of Justice, 2018) :

- That Units 26164 and Unit 74455, which are within the body of GRU, are the units which plan the manipulations against the 2016 Presidential Elections of the US and that the 12 GRU officers, whose full names and ranks are stated, are the planners and practitioners of these operations in person.

- That the earliest date determined regarding the beginning of the operations in question is March 2016 and thousands of e-mail communications are disclosed through the social media and internet accounts opened on behalf of fake persons named "DCLeaks" and "Guccifer 2.0" and via other mass media organs.

- That the domain addresses of these accounts and internet addresses are obtained by using fake methods from the US to avoid any association with the RF government,

- That the GRU is identified as "X-Agent" in the e-mail communications obtained within the scope of the manipulation activities and e-mail communications were leaked by means of these malwares and the budget used in these operations are supplied to the GRU staff in question through "Bitcoin" mining.

On the other hand, it can be argued that the election propaganda process of the US Democratic Party was partially affected by these disclosures. Debbie Wasserman Schultz (The chairwoman of DNC) and some senior officials resigned, the position of the Democratic Party's other presidential candidate, Senator Bernie Sanders, was strengthened and his nomination was continued for an additional period, the hand of Republican Party was strengthened to be used against the Democratic Party and the name of Clinton has become disputable and worn out (Turk Internet News Website, October 11, 2016). However, it can be argued that the negative effect of the e-mails disclosed as a result of these cyber-attacks is the most important factor that brought Trump's victory against Clinton is an assertive consideration. At this point, it must be taken into consideration that some of the circles in the United States have been bringing the cyber-attacks into question constantly in order to wearing out and oppressing Trump after his victory in elections and using them against Trump.

2. THE RUSSIAN INTELLIGENCE ORGANIZATION AND ASSESSMENT OF GRU'S PERFORMANCE IN MANIPULATION OF US PRESIDENTIAL ELECTIONS 2016

GRU, FSB (Federalnaya Slujba Bezopasnosti / Russian Federal Security Service), SVR (Sluzhba Vneshney Razvedki / Russian Intelligence Service) and FSO (Federalnaya Sluzhba Okhrany / Federal Protection Service) are in the organization of the Russian Intelligence Services (RIS). The SVR is responsible for the external intelligence activities of these services and the FSO, which is responsible for managing the secure and secure communication of the FSB, high-level and confidential communications responsible for internal intelligence activities, is directly affiliated to the RF President. GRU is a part of the Ministry of Defense and serves under the control of RF Armed Forces (See at more; Darıcılı, Autumn 2017: 128-130).

A concrete example to elaborate the issue is that it is the FSB's duty to monitor, track and gather intelligence on the activities of the separatist Circassian / Chechen groups, jihadist terrorist organizations or organized crime syndicates in the RF. Another task of the FSB is to counter the espionage activities targeting the RF. This counteraction is called the counter / espionage work and involves the aim of preventing operations against RF from foreign intelligence services. In this context, it is FSB's duty to counter cyber-attacks against RF and to ensure the cyber security of the country (See more at; The Centre for Counterintelligence and Security Studies, 2018).

SVR is the foreign intelligence service that RF established as a continuation of the KGB in order to carry out the espionage activities abroad. SVR is a key actor in the fulfilment of foreign intelligence needs of RF, together with GRU. SVR gathers

intelligence on military, political, biographical, economic, social, transport, communication, science and technology for the government it targets. For example, RF's operations aiming at detecting the military capacity of the US in a region of the world or predicting the outcome of elections in Hungary or in Turkey is managed by the SVR. In terms of cyber security strategy, it is among the tasks of SRV to plan cyber espionage operations targeting a country's science and technology capacity on behalf of the RF (See more at; Staar, 2006: 39-57).

As stated, while the FSB fulfils the task of meeting the internal intelligence needs of the RF, the GRU is the main actor in cooperation with the SVR in meeting the foreign intelligence needs of RF. GRU is a military intelligence agency operating under the Russian General Staff. The GRU, which is affiliated to the Red Army in the time of the USSR, is the intelligence service of the RF with the largest number and capacity under the Russian Armed Forces. In addition to military and foreign intelligence issues, GRU has the power to gather intelligence in all areas related to national security. In terms of cyber security, the main tasks of GRU are to conduct counter-espionage activities against foreign service-based cyber operations targeting Russian military capacity and to plan cyber operations against the military capacity of the target country (See more at; The Centre for Counterintelligence and Security Studies, 2018).

At this point, GRU's successful performance during the Ukrainian intervention of the Russian Armed Forces in 2014 was demonstrated. GRU's contribution to this multi-faceted hot conflict performance, called the Gerasimov Doctrine or Hybrid War Concept, should be further examined in the context of the purpose of demonstrating the success of GRU in manipulating the US Presidential Elections. The failure of GRU during the Georgian Intervention in 2008 seriously undermined the reputation of this intelligence organization compared to other RISs. This deterioration ended in 2011 when Igor Sergun was appointed as the director of GRU. GRU has been highly successful under the direction of Sergun, especially in the planning of cyber operations before and during the Ukrainian intervention, as well as in the coordination of the special forces and the activities of pro-Russian separatists. GRU's superiority after the Intervention of Ukraine compared to other RISs has made GRU the main intelligence service that dominates the foreign operations of RF. With increasing successes and thus developing personnel, budget and technology investments, GRU has evolved into a highly sophisticated service that can organize global cyber operations (See more at; Galeotti , 2016).

As we have mentioned, it was aimed to have a broad systematic structure based on espionage operations arranged as cyber-attacks in terms of intelligence gathering intelligence as part of the plans supported by Putin with the influence of the prestige, which was achieved after the GRU 2014 Ukraine Intervention, besides HUMINT

(Human Intelligence), SIGINT (Signal Intelligence), and other intelligence total techniques. The RF aimed at meeting the economic, financial and technological intelligence needs which are vital in terms of economic development of the Russian society and energy security, ensuring the security of the country, carrying out manipulative cyber operations against hostile countries as provided in the example of US Presidential Elections whenever needed with this organization (See more at; Hagestad, 2013).

The success of the GRU in manipulative cyber operations against the 2016 US Presidential Elections can be analysed in terms of intelligence techniques with regards to the determinations stated in the following;

- GRU has regained its shaken prestige in the Intervention Against Georgia with its multi-faceted warfare performance which is called as Gerasimov Doctrine according to some and Hybrid War Concept according to others which it performed during the Intervention Against Ukraine with the successful directorate of the Igor Sergun. With the positive atmosphere created by this successful contribution, GRU, which has been consistently supported by the RF Presidency in terms of budget, personnel and technology, has reached the ability to manipulate the 2016 US Presidential Elections.

- As clearly demonstrated in the Muller Investigation, GRU has commissioned staff with highly professional level intelligence planning and sophisticated software development capabilities to intervene in the US Presidential Elections in special units named Units 26164 and Unit 74455. Thus, an operational activity that requires software development and clandestine operation planning competence has been successfully planned.

- As uncovered in the Muller Investigation, the GRU has made the most of the anonymous structure of the cyber space in order to prevent the manipulative activities from being associated with RF. Fake internet and social media accounts were purchased from outside of RF, and the budget required for these operations was provided by "Bitcoin Mining" which is a crypto method again. At this point, the US counter / espionage systematic, which is responsible for uncovering the RF-based intelligence operations, was misled and the uncovering of the operation was prevented.

- All e-mails procured to manipulate the US Presidential Elections were carried out using a target-oriented phishing method known as "spread phishing". As an operational hacking method, phishing concept is a password stealing method which is derived from the phrase of “Password Fishing”. In this type of attack, copies of generally known web pages are made and the hosts file on your computer is changed

so that you can enter your username and password manually. After this stage, the user name and password combination that you enter to log in to the fake page will be sent to the address specified by the attacker. Phishing attacks can be done via the web page or via e-mail. In order to implement this method, it is necessary to know the hundreds of DNC managers and members' e-mail addresses, to determine who has a more important position among many targets and to plan a target-oriented "spread phishing" after this detection. It is clear that GRU has made a serious preparation much earlier than 2016 March, when GRU has started operation, and made planning by narrowing target. In such a planning, it is understood that GRU has already created a serious archive information using HUMINT methods on subjects such as status, habit, and position of the target persons in DNC.

On the other hand, in addition to the GRU's achievements, it can be argued that the deficiencies of the US counter/espionage systematics created under the leadership of the FBI paved the way for the intervention of the US Presidential Elections.

3. US COUNTER / ESPIONAGE ORGANIZATION AND EVALUATION OF THE PERFORMANCE OF THE FBI IN MANIPULATION PROCESS OF 2016 PRESIDENTIAL ELECTIONS

Counter-espionage activities have played an important role in the US national security system since the foundation of the US. The establishment of espionage and counter / espionage units of the US was ensured during the independence war against English Empire with George Washington's personal initiatives and within the US armed elements. The activities of the FBI's counter / espionage department officially started in 1917. The US counter / espionage systematic, which experienced a rapid development within the framework of resisting against the German and Japanese intelligence activities during the World War II, laid the foundations of today's institutional structure after the effective resistance against the espionage activities of the Soviet Block during the Cold War (See more at; Reagan, 2005).

In the US intelligence structure, the concept of counter-espionage has a number of definitions that are parallel to each other and which is prepared by the US intelligence services within the scope of their area of responsibility. The approach in Executive Order 12333 published in 1981 is important as an official definition. Counter/intelligence means "*Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities*" (See more at; The Office of The Director National Intelligence, 1981).

There are a dual resistance strategy in the US counter/espionage system as in the national system of other states. This strategy, which we can call active resistance and passive resistance, is the basis not only for the US but also for all national counter/intelligence strategies. In this respect; "*all of the countering activities performed by official institutions*" are called active resistance. The main active resistance factor in the US counter / espionage systematic is any activities carried out by the FBI to protect national interest of the US against foreign intelligence services. Passive resistance can be defined as "*intelligence notion (awareness) which stems from the traditions and social characteristics in the society or which is raised through educational activities*". The mechanisms of denunciation, the development of a sense of responsibility stemming from education and social traditions, the educational activities carried out by the intelligence services, can be counted as passive resistance elements.

The FBI is the federal agency of the US in the field of counter-espionage, which manages judicial control processes. The FBI is the intelligence organization that meets the US's internal intelligence needs and which counters other states' spying operations against the United States (Darıcılı, 2017b: 96). The FBI's official site has some important determinations and assessments regarding the FBI's counter / espionage activities. According to this, the FBI defines the current counter-espionage activities as a structure aiming at stealing the most valuable secrets of the US society which is a more complicated definition than the Cold War period. As it is understood from this definition, the US intelligence system followed a strategy based on the security of the state in the post-Cold War period, as in the Cold War period. On the other hand, it is stated that the activities of the FBI's counter / espionage department officially started in 1917 and the activities of this department, which is mainly active against the espionage activities of the Soviet Bloc during the Cold War period, have evolved into a much more complicated structure due to the changing threat sources (See more at; FBI, 2018).

Some additional organizations have been established in the US counter / espionage system on sectoral and specialization to protect the strong position of the US as a global technology and commercial power in the international system. For example, a unit named OICI (The Office of Intelligence and Counterintelligence) has been established within the DOE (The Department of Energy) in order to prevent the activities of foreign intelligence services against the national energy sector of the US. The United States aimed to counter the espionage activities against energy projects and facilities, which are large-scale, widespread and therefore very difficult to control, by the cooperation of the specialized organization OICI and the FBI, which is authorized at federal level. As a result, OICI, which was established within the strategy of decentralization of specialization and authorities in the intelligence system, has an important role in countering intelligence activities of the hostile

intelligence services against the US energy sector (See more at; Congressional Research Service, 2005).

Similarly, for instance, another counterintelligence structure based on a decentralized understanding is TFI (The Office of Terrorism and Financial Intelligence). This service is subject to USDT (The Department of the Treasury). The TFI was established in 2004 being responsible for monitoring the financial activities of terrorists, groups, drugs and organized crime organizations (See more at; U.S. Department of Treasury, 2018).

In this framework, it can be stated that FBI, which holds the planning of the federal counter / espionage activities and the legal control authority regarding this process, is the main actor in US counter / espionage systematic, while organizations such as OICI or TFI are secondary actors operating in their area of responsibility. There is close coordination between these services and the FBI. The FBI's coordination function regarding counter / espionage is similarly in question with the US Department of Defense and DHS (See more at; FBI, 2018).

The fact that the US security and intelligence services have revealed the manipulative activities of the GRU in detail by revealing the full names of the units and officers involved in this activity and the fact that an indictment has been prepared in this regard is not very meaningful in terms of the counter / espionage technique. Since this type of work took place after the completion of the process, it should no longer be considered as a counter / espionage activity but as a judicial process. However, as revealed in the Muller Investigation, that the US intelligence and security services could uncover all of the GRU's activities in detail is the indicator that the CIA, which is responsible for US foreign intelligence operations, took position against the Russian intelligence and security services in a short period and could create a HUMINT and SIGINT gathering systematics.

CONCLUSION

The manipulation processes of the elections, which were generally carried out through budget, media support and pressures until today, has reached a new dimension with the RF's manipulation of the US 2016 Presidential Elections through disclosing the e-mails of the members of the Democratic Party, which it procured within cyber espionage activity, through internet and social media. The reason for the RF's planning a process of an election manipulation with such a cyber operation is directly related to the rapid civilization, commercialization and globalization of the Internet in the 2000s and penetration of the it into all areas of our lives.

The GRU quickly recovered from the negative impact of the failure in the Intervention Against Georgia in 2008 with the successful directorate of the Igor

Sergun, who has become the director of the GRU in 2011. In this framework, the GRU has been highly successful in planning cyber operations before and during the 2014 Intervention against Ukraine. The GRU's superiority after the Intervention of Ukraine compared to other RISs has made GRU the main intelligence service that dominates the foreign operations of RF. The GRU has evolved into a highly sophisticated service that can organize global cyber operations with increasing successes.

The GRU directorate has begun to closely monitor the manipulation and provocation opportunities provided by the social media in parallel with its developing budget, personnel and technology investments. The GRU has established special units, where employees have the competence to make intelligence planning and software development in order to intervene in the US Presidential Elections. Within the scope of the activities of these units has accomplished the confidentiality of the intelligence activities in question through fake internet and social media accounts opened outside of the RF and with the budget they procured by doing "Bitcoin Mining". At this point, the US counter / espionage systematic, which is responsible for uncovering the RF-based intelligence operations, was misled and the uncovering of the operation was prevented. E-mails of many DNC directors and members were procured using a target-oriented phishing method known as "spread phishing". In addition, prior to March 2016, which was reported as the earliest start date for this operation, the GRU also planned a serious preparatory process in order to obtain the e-mails of persons with the most striking information about the Democratic Party campaign process by narrowing the target.

On the other hand, the US counter / espionage systematic, dominated under the leadership of the FBI, failed to uncover the operational activities of the RF in time. The main reason for this failure is that the US counter / espionage systematic, which has wide range of responsibilities and which includes different institutional structures within its body, was not able to achieve the coordination between these institutions successfully. It can be evaluated that the US intelligence and security units did not adequately analyse the steps taken by GRU to increase its cyber capacity after 2014. It can be argued that the US intelligence and security units have considered that the SVR can design such a cyber operation rather than the GRU, which is weak in terms of power before 2014, and that it did not monitor the activities of the GRU adequately. - Another reason of the failure is related to unfavourableness of the close monitoring of the election campaigns of the Democrat or Republican Party by the FBI during the election process for the US democratic traditions. At this point, it can be argued that the FBI avoided taking initiative to protect the contact information of the people involved in the Democratic Party election process in order not to cause any complications during the election campaign and in this respect, laid the foundations for the operation of the GRU.

Accordingly, the failure of the FBI in uncovering and preventing the cyber operations against the 2016 US Presidential Elections can be analysed in terms of intelligence techniques with regards to the assessments stated in the following;

-As it is seen, the US counter / espionage systematic has a large area of responsibility. This is associated with the US being a major economic, political and technological power at the global level. For this reason, the US cannot only be the target of the RF or the People's Republic of China (PRC), but also the intelligence activities of many allied states. In this context, it can be claimed that the FBI is not able to make a proportional activity focalization and narrowing down of the target priorities and thus it left the persons within the Democratic Party campaign systematics unprotected against the intelligence activities of the GRU.

-The US counter-espionage strategy has made a choice of narrowing down the area of responsibility of the FBI, by establishing structures that carry out their own counter-espionage activities based on sectoral and specialized areas such as TFI or OICI, depending on the diversified threat foci over time. Although this seems to be a successful strategy in the first stage, it is clear that this strategy causes complications if the coordination between institutions is not achieved effectively.

-It can be argued that the US did not adequately analyse the steps taken by GRU to increase its cyber capacity after 2014. It is natural for SVR to be effective in the foreign operations of the RF instead of GRU, which is weak in pre-2014 period. At this point, it can be claimed that the FBI is not able to adequately monitor the activities of the GRU, considering that the organization which can plan such a cyber operation would be SVR based instead of GRU.

-The close monitoring of the election campaigns of the Democrat or Republican Party by the FBI during the election process can be considered as unfavourable for the US democratic traditions in the first place. Based on this evaluation, it can be argued that the FBI avoided taking initiative to protect the contact information of the people involved in the Democratic Party election process in order not to cause any complications."

As it is tried to be analysed with details in our study, it is obvious that the RF tried to intervene in the 2016 Presidential Elections by means of the GRU, which has become the main intelligence structure in the post 2014 period. It is clear from the above-mentioned evaluations that the US could not uncover these operations in a timely manner by means of the FBI, which is the main intelligence service responsible for the counter / espionage activities. In this sense, it can be argued that there is the success of the GRU in terms of intelligence and the failure of the FBI. However, it is quite assertive to say that this operation fully affected the results of the

2016 US Presidential Elections in terms of the results, even if it is considered as a success for GRU in terms of planning within the scope of intelligence techniques.

Some senior officials of the DNC resigned as a result of the disclosures, the position of the Democratic Party's other presidential candidate for nomination, Senator Bernie Sanders, was strengthened and the hand of Republican Party was strengthened to be used against the Democratic Party and the name of Clinton has become disputable. However, it is an incorrect conclusion to think that the negative effect of the e-mails disclosed as a result of these cyber-attacks is the main factor that brought Trump's victory against Clinton. At this point, it is obvious that some of the circles opponent to Trump have been bringing these claims into question constantly in order to wearing out and oppressing him during his presidency.

Another important result of the RF intervention in the 2016 US Presidential elections is the fact that social media has become a new generation and the most effective information warfare instrument. The Internet and the use of social media developed in this context have become indispensable elements of our lives and security approaches. The sphere of influence has expanded to all areas of social, economic, commercial, scientific, cultural and daily life with the increasing use of social media in the daily life. The nature of the social media, which allows the global circulation of unique and different contents at low cost, is considered as a new means of manipulation by the intelligence services.

On the other hand, the opportunities and facilities created by social media have led to radical changes in political, military, security and economic life beyond our daily life with the potabilization of computer and proliferation of smartphones. The digital domain called cyber space has become a new generation information battlefront for the intelligence services as a result of the emergence of the Internet, developments in network technologies and new opportunities created by social media. The most recent and concrete example of this battlefront was observed between the US and the RF intelligence services in the context of intervention processes against the US 2016 Presidential Elections.

REFERENCES:

Başbaşoğlu, A.rif (2011). "Füze Savunma Sistemi ve Türkiye", Orta Doğu Analiz, 3 (34), pp. 74-79.

Bıçakcı, Salih (Winter 2014). "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", Uluslararası İlişkiler, 10 (40), pp. 101-130.

Bıçakcı, Salih. (2013). "21. Yüzyılda Siber Güvenlik", Bilgi Üniversitesi Yayınları, İstanbul.

CNN International (June 2, 2017). "Putin: 'Patriotic' Russian hackers may have targeted US election", https://edition.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html, (accessed; October 10, 2018).

Congressional Research Service/The Library of Congress (2005). "Counterintelligence Reform at the Department of Energy: Policy Issues and Organizational Alternatives", Washington, DC, https://fas.org/sgp/crs/intel/RL31883.pdf, (accessed; October 10, 2018).

Darıcılı, A. Burak (2017a). "Demokrat Parti Hack Skandalı Bağlamında Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Analizi", Yıldırım Beyazıt Üniversitesi Uluslararası Çalışmalar Dergisi (ULİSA), 1 (1), pp. 1-24.

Darıcılı, A. Burak (2017b). "Siber Uzay ve Siber Güvenlik; ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi", Dora Yayıncılık, Bursa.

Darıcılı, A. Burak (Autumn 2017). "Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi", Journal of Social Sciences of the Turkic World (BİLİG), 83, pp.121-146.

Department of Homeland Security (2016a). "Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity", Washington, DC, https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity, (accessed; October 5, 2018).

Department of Homeland Security (2016b). "Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale", Washington, DC, https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary, (accessed; October 5, 2018).

FBI (2018). "Counterintelligence", https://www.fbi.gov/investigate/counterintelligence, (accessed; October 9, 2018).

Galeotti, Mark (2016). "Putin's Hydra: Inside Russia's Intelligence Services", European Council on Foreign Relations (ECFR), pp. 1-19, https://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services, (accessed; September 26, 2018).

Keskin, Mustafa (2016). "ABD'nin Müdahaleci Dış Politikası; Latin Amerika Örneği", Barış Araştırmaları ve Çatışma Çözümleri Dergisi, 4 (1), pp.70-88.

Khanna, Parag (2008). "Yeni Dünya Düzeni", Trans; Akbaş, Elif, Nihan; Pegasus Yayınları, İstanbul.

Mowthorpe, Matthew (2005). "The Revolution in Military Affairs (RMA): The United States, Russian an Chinese Views", Journal of Social, Political and Economic Studies, 10 (2), pp. 137-153.

NATO Strategic Communications Centre of Excellence (2016). "Social Media as A Tool of Hybrid Warfare", Tallinn, http://www.stratcomcoe.org/download/file/fid/5314, (accessed; October 14, 2018).

Office of the Director of National Intelligence (2017). "Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution", Washington, DC, https://www.dni.gov/files/documents/ICA_2017_01.pdf, (accessed; October 7, 2018).

Pero Del, Mario (2001) "The United States Activities on Pyshological Warfare 1948-1955", 87(44), pp.1-31

Reagan L, Mark (2005). "Introduction to the USA Counterintelligence", USA, https://www.hsdl.org/?view&did=460369, (accessed; September 28, 2018).

Skidmore E. Thomas and Smith H. Peter (2005). "Modern Latin America", Oxford University Press, 6. Edition, New York.

Sputniknews Portal (December 29, 2016). "Beyaz Saray ABD, 35 Rus diplomatı 72 saat içerisinde sınır dışı edecek", https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi/, (accessed; September 23, 2018).

Sputniknews Portal (December 30, 2016). "Putin'den ABD'ye yanıt: Biz hiç kimseyi sınır dışı etmeyeceğiz.", https://tr.sputniknews.com/rusya/201612301026565257-putin-abdye-yanit-biz-hic-kimseyi-sinir-disi-etmeyecegiz/, (accessed; September 23, 2018).

Staar, F. Richard and Tacosa, A. Carliss (2014). "Russia's Security Services", Mediterranean Quarterly, 15 (1), pp.39-57.

The Centre for Counterintelligence and Security Studies (2018). "Russia's SVR/FSB/GRU Intelligence Services", https://cicentre.site-ym.com/page/191, (accessed; October 20, 2018).

The Office of The Director National Intelligence (1981). "United States Intelligence Activities (Federal Register Vol. 40, No. 235 / December 8, 1981, amended by EO 13284 / 2003, EO 13355 / 2004, and EO 13470 / 2008)", https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-12333, (accessed; October 17, 2018).

The Department of Justice (2018). "Case 1:18-cr-00032-DLF Document 1 Filed 02/16/18 Page 1 of 37 (The Report of Muller Investigation)", Washington, DC https://www.justice.gov/file/1035477/download, (accessed; October 17, 2018).

Turk Internet News Website (October 11, 2016). "Beyaz Saray, Rusya'nın Hackleme Operasyonuna Cevap Verileceğini Açıkladı", http://www.turk-internet.com/portal/yazigoster.php?yaziid=54247, (accessed; October 14, 2018).

U.S. Department of Treasury (2018). "About Terrorism and Financial Intelligence, Washington,DC,https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx, (accessed; October 10, 2018).

Williams, M.Eric (2012). "Understanding U.S.-Latin American Relations: Theory and History", Routledge.