Uludağ Journal of Economy and Society / B.U.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi Cilt / Volume 37, Sayı / Issue 2, 2018 ss./pp. 1-10

CYBER ATTACKS AGAINST TURKEY RIGHT AFTER SHOTTING DOWN RUSSIAN SU-24 AIRCARAFT*

Ali Burak DARICILI*

ABSTRACT

Russian Federation (RF), which has an effective cyber attack capacity at the global level, does not hesitate to use this capacity as a pressure instrument for the states in which it has problems in foreign policy. Examples of this policy include cyber attacks allegedly carried out against Estonia in 2007, Georgia and Lithuania in 2008, and Kyrgyzstan in 2009. November 24, 2015 Date of Turkish F-16 of airspace after the lowering of a Russian Su-24 aircraft that violate December 14, 2015 date in Turkey's mainly financial institutions that target "DDoS" attacks include similarities with the specified cyber attacks On the other hand, it should be taken into consideration that even though the attacks can be claimed to be of RF origin, the cyber space can easily hide the real identity of the attacker due to its anonymous structure. In this context, it may never be clear that such cyber attacks are planned by RF. This is due to the anonymous structure of cyber space. However, in this article, it will be tried to analyze why cyber attacks are likely to be caused by RF.

Key Words: Russia, Turkey, Cyber Attacks, Cyber Strategy, Cyber Security.

---

* This article is derived from the thesis under the name of "Comparative Analysis of Cyber Security Strategies of the United States and the Russian Federation" written by A. Burak DARICILI in Uludag University, Institute of Social Sciences, International Relations PhD Program.

* *Dr. Ali Burak DARICILI, Bursa Technical University, Faculty of Human and Social Sciences, Department of International Relations, Bursa / Turkey, E-Mail: ali.daricili@btu.edu.tr*

Ali Burak DARICILI

RUS SU-24 SAVAŞ UÇAĞININ DÜŞÜRÜLMESİ SONRASINDA TÜRKİYE'YE YÖNELİK SİBER ATAKLAR

ÖZ

Küresel düzeyde etkili bir siber saldırı kapasitesi sahip olan Rusya Federasyonu (RF), bu kapasitesini dış politikada sorun yaşadığı devletlere yönelik olarak bir baskı enstrümanı olarak kullanmaktan çekinmemektedir. Bu politikanın örnekleri arasında RF'nin 2007 yılında Estonya'ya, 2008 yılında Gürcistan'a ve Litvanya'ya, 2009 yılında ise Kırgızistan'a yönelik gerçekleştirdiği iddia edilen siber saldırılar gösterilebilir. 24 Kasım 2015 tarihinde Türk F-16'larının hava sahasını ihlal eden bir Rus Su-24 uçağını düşürmesi sonrasında 14 Aralık 2015 tarihinde Türkiye'nin özellikle finans kurumlarını hedef alan "DDoS" saldırıları ise belirtilen siber ataklar ile benzerlik içermektedir. Öte yandan söz konusu saldırıların RF kaynaklı olduğu kuvvetle iddia edilebilecek olsa bile, siber uzayın anonim yapısı nedeniyle saldırganın gerçek kimliğini rahatlıkla gizleyebilmekte olması da dikkate alınmalıdır. Bu kapsamda bahse konu siber saldırıların RF tarafından planlandığı hiçbir zaman netleşemeyebilecektir. Bu durum siber uzayın anonim yapısından kaynaklanmaktadır. Bununla birlikte, bu makale de bahse konu siber atakların yapısı ve bu ataklar kapsamında ortaya çıkan bazı emareler ortaya konmak suretiyle, belirtilen siber saldırıların neden RF kaynaklı olma ihtimalinin yüksek olduğu analiz edilmeye çalışılacaktır.

Anahtar Kelimeler: Rusya Federasyonu, Türkiye, Siber Saldırı, Siber Strateji, Siber Güvenlik.

INTRODUCTION

In the beginning of the 1980s, RF introduced the initial planning of adapting network technologies to conventional military power. The Union of Soviet Socialist Republics (USSR) during the Afghanistan War between 1979-1989 was not successful enough to implement psychological warfare techniques and to ensure effective communication between field troops in Afghanistan and the headquarters in Moscow. (Heickerö, 2010: 15). In this context, in the years in question, the program of the Revoluation in Military Affairs program was initiated by Marshal Nikolai Ogarkov on the elimination of the weaknesses of the USSR Army. (Darıcılı, 2017: 122)

Similarly, during the Chechen War of 1994-1996, RF failed to counteract the new generation of propaganda efforts from the internet. In other words, as a result of these propaganda processes, RF has been deemed as a war crime committed state in the Chechen War by the international public. (Darıcılı, 2014: 4) Due to these developments, the Russian security and military bureaucracy started to develop plans to adapt the technological developments based on cyber space from the 1990s to the hard power.

After the North Atlantic Treaty Organization (NATO) began to bombard Serb forces in the former Yugoslavia in 1999 as the first result of these plans, the Serbian and Russian hackers ordered the military communication systems of the Pact member states to Cyber attacks on their structures. (Bıçakçı, 2013: 50). On the other hand, since this period, RF has begun to make serious efforts in the 2000s in order to increase cyber attack capacity. As a result of the strategy followed, RF has become one of the most important cyber forces in the international system. Wanted to use as a pressure and sanction tool at the point of. In this respect, it is claimed that cyber attacks were planned by RF in 2007 in Estonia, Georgia and Lithuania in 2008, Kyrgyzstan in 2009 and finally in Ukraine in 2014. (For more information, see Darıcılı, 2014: 4-5). However, on November 24, 2015 Turkish F-16 of airspace after dropping a Russian Su-24 aircraft violators on December 14, 2015, especially financial institutions that target Turkey's "DDoS" can be suggested that contain similarities with the specified cyber attacks on the attack.

CYBER ATTACKS AGAINST TURKEY AFTER SHOTTING DOWN RUSSIAN SU-24 AIRCRAFT

On the morning of November 24, 2015, the news that the Turkish F-16s had dropped a Russian Su-24 airplane that violated the airspace had a shocking effect all over the world. This event deepened in a short time, reached serious proportions between Turkey and the beginning of the RF has created political tensions. This political tension, with the 12.00 December 14, 2015, as against Turkey Distributed Denial of Service (DDoS) moved into a new phase with the attacks, has caused deepening tension in relations between two countries. It said the cyber attacks "tr" bandwidth extension systems that use targeted Turkey's banking and finance, public institutions, aimed to eroding of the e-government system constitutes critical infrastructure (Türk Internet Sitesi, 2015).

On the 23rd of December 2016, a video was broadcasted by the Anonymous Hacker Group about the attack. Posted in Videos claimed that Turkey supports Islamic State of Iraq and Syria (DAESH), Turkey gets oil illegally from DAESH and terrorists from DAESH are being treated in Turkey (IB Times Internet News, 2015). It is also claimed that this disclosure is part of the false flag operation[1] planned by the Russian Service Services (RIS).

Binali Yildirim, Minister of Transport and Communications of Turkey at that time, who was involved in the attacks, said in a statement on 24 December 2015. Accoridng to him; "*Information Technologies and Communication Authority (BTK) and Telecommunications Communication Presidency (TIB) intervened immediately to these attacks, until the 17th of December, this event is continuing, it is not easy at the first time to determine which country backed this attack, such a determination is very detailed and laborious, the attacks are planned from abroad, the National Cyber Incidents Center (USOM) plays an important role in the fight*" (HaberTürk Internet Haber Portalı, 2015).

---

1 False Flag Operation: is the name given to the secret plans designed by the secret organizations or the intelligence services to provoke the public, or to steer the public by showing them as a subversive (subversive) purpose, conducting some of their activities and operations as the target people.

Turkey in response to these attacks, on the first day of the attacks overseas and cut internet traffic from abroad "tr" extension is blocked access to the site. At this stage, Cyber-Event Fighting Teams (SOME) played an important role (Haberler İnternet Haber Portalı, 2015). Another measure was taken as a temporary copy of the attacked DNS servers to the Netherlands. Thus, the size of the attacks was tried to be alleviated. The attacks, however, indicated that Turkey's partly from the cyber security strategy, cyber defense is still extremely poor resistance, revealed that it is messy and unplanned. For example, no official authority has made an explanation of the nature of the attacks over the attacks, almost a week later in the period in question. This has led to serious disinformation during cyber attacks. It has been seen that the METU, BTK, TIB and SOMEs have developed countermeasures against the attacks and their respective fields of activity. It can be said that METU has demonstrated a successful performance in contrast to the criticisms made during the attacks. However, when it comes to cyber security in the country, it is also clear that the authority of the METU DNS group should be transferred to the relevant state institutions. In this regard, an urgent compromise should be reached between official authorities and METU, and the country's cyber security should be transferred to the relevant state institutions.

In addition, the said cyber attacks are adequately discussed the agenda of Turkey. This situation is related to the unfamiliarity of the Turkish public to the concept of cyber security. For Turkish internet users, the internet basically means the use of social media and e-mail communication (BBC News, 2015).

It is still quite difficult to make a clear assessment of the damage caused by the attacks. For example, it is common for Western countries to make public statements by the agencies involved in dealing with the cost of the damage resulting from such attacks or virus outbreaks. However, there is not yet any institution to carry out such a study in our country. After the attacks, it should be noted that in December 2015, when attacks continued, 10% visitor losses were reported on sites with high visitor traffic "com.tr" (Türk Internet Sitesi, 2015).

On the other hand, it is unclear whether a cyber espionage activity against state institutions has been carried out during these cyber

attacks, which are alleged to have been caused by RF. In this context, it will be seen whether the state's strategic information is leaked from Turkish official institutions and organizations during the cyber attack.

With the said measures taken against cyber attacks, and other matters on a point of inactivation of this attack it is related to the weakness of Turkey's website infrastructure. Normally, it is expected to produce a response in times of an attack of such magnitude, and in this case the effect of different advanced attack in Turkey was lower. Today, Turkey's fiber infrastructure is 250,000 kilometers. However, this figure is comparable to that of Portugal, 4 million km. should be. As well as internet use in Turkey is quite expensive. Therefore, server-side traffic remains low. 1Gbps per server with traffic in Europe, may be considered as 10 Mbps in Turkey.

CAUSES ASSOCIATING CYBER ATTACKS WITH RF

It is almost impossible to say who plans a DDoS attack. But this DDoS atttack can be evaluated form some aspects. For example, at least 400,000 web sites were affected by these attacks and these sites were just belong to e-government system, public universities and financial instituitons. At that time, there was an ongoing high tension between RF and Turkey because of shotting down Russian SU-24. Also, This cyber attack did not target the entire internet system in Turkey, only official internet sites were targeted by these attacks. Finally, RF has bad reputation in similar kind of DDoS attacks (The Telegraph Online News, 2015).

It can also be stated that a more technical approach was to prepare attacks in a simple format, to hide the background of the incident and to attempt to show the attack as an individual hacker group attack. Within the scope of the technical evaluations mentioned below, it can be assumed that these attacks could be carried out with the support of RF (Türk Internet Sitesi, 2015).

- It is technically not possible for the servers to be operated by individuals for a long time.

- In order to produce 30 gbps attack traffic in these attacks, it requires continuous traffic between 5-10 GBps.

- The fact that the attack has a capacity of 276,000 different addresses and 30-40 gb size from time to time; considering this huge capasity, it can be easily evaluated that this DDoS attack can be planned with just a support form a state organization.

In terms of international relations discipline of cyber attacks against Turkey include similar features with cyber attacks towards Estonia, Georgia, Ukraine, Kyrgyzstan and Lithuania planned allegedly by RF. Like attacks against these states. "DDoS" attacks towards Turkey targeted Turkish critical infrastructure. The beginning of the attack came on the 24th of November 2015 just after shotting down RF Su-24. From this point, it can be said that RF wanted to corner Turkey not only with diplomatic pressure and economic measures but also this DDoS attack.

At this stage the influence and power of RF cyber capacity, when Turkey is also considering said multi-headed and unprepared structure in cyber defense strategy, RF is continued until a stage where the cyber attacks against Turkey, thus testing the cyber capacity in Turkey he also does not want more meat to deepen existing tensions in relations with Turkey could only assess opportunities and also wants to demonstrate its cyber power (Yinanç, 2015)

RESULT

The security of states is now highly dependent on cyber space-based technologies. After the 1990s, internet technology and civilization, together with network technology-centered innovations, cover the entire field of our lives. In this context, critical infrastructures, where public services and security activities are provided, have also begun to be managed within a highly sophisticated software program.

However, states have also realized that if there is no technology in cyberspace space, this situation will create serious security weakness. As a result, states have started to invest in cyber defense and attack capacities and endeavored to develop effective cyber security strategies. In this context, with the strategies and plans put forward after the 2000s, RF has become an important actor dominating the cyber space. In this respect, RF does not hesitate to use its strong and

aggressive activity in cyber space against the countries in which it has problems in foreign policy.

The goal of RF is to have a strong and aggressive cyber security capacity. The RF is mainly based on negative experiences during the Afghanistan War between 1979-1989. In this context, the USSR did not succeed enough in the implementation of psychological warfare techniques during this war and to ensure effective communication between the field troops in Afghanistan and the headquarters in Moscow. In this context, the program called RMA (Revoluation in Military Affairs) was taken up by Ogarkov in order to eliminate the weaknesses of the USSR Army. Similarly, during the Chechen War of 1994-1996, RF failed to counteract the new generation of propaganda efforts from the internet. In this development, the political will of the RF and the security bureaucracy helped the Internet to understand the importance of Internet-based technologies much earlier than in other states.

As mentioned, RF has frequently used cyber opportunities against the states with which it has problems in international relations with the cyber-attack capacity it reached after 2000s as a method in foreign policy strategy. In this respect, cyber attacks targeting Estonia in 2007, Georgia and Lithuania in 2008 and Kyrgyzstan in 2009 are remarkable. Similarly, in Turkey, in particular financial institutions targeting the 14 December 2015, "DDoS attacks allegedly planned by the RF can be claimed.

REFERENCES

Bıçakçı, Salih (2013): "21. Yüzyılda Siber Güvenlik", Bilgi Üniversitesi Yayınları, İstanbul / Türkiye.

BBC News (2015): "Türkiye'ye Siber Saldırının 10 Günü: Ne oldu?", https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan, (accessed date; 25.04.2016).

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

Darıcılı, A. Burak (2014): "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar", Uludağ Üniversitesi Sosyal Bilimler Dergisi, 7 (2), pp.1-16.

HaberTürk Internet Haber Portalı (2015): "Binali Yıldırım'dan ODTÜ açıklaması", http://www.haberturk.com/ekonomi/teknoloji/haber/1171682-binali-yildirimdan-odtu-aciklamasi, (accessed date; 25.11.2018).

Haberler İnternet Haber Portalı (2015): "Türkiye'ye Siber Saldırının Arkasında Ruslar Var", http://www.haberler.com/turkiye-ye-siber-saldirinin-arkasinda-ruslar-var-8006069-haberi/, (accessed date; 25.11.2018).

IB Times Internet News (2015): "Anonymous: Turkey reeling under cyberattack as government and banks websites paralysed", https://www.ibtimes.co.uk/anonymous-turkey-reeling-under-cyber-attack-government-banks-sites-paralysed-1534984, (accessed date; 24.12.2018).

Türk İnternet Sitesi (2015): "6. Gününde Nic.tr Saldırısı Sürüyor Ama Açıklama Yok-Onun Yerine" Yorumlar Var.., https://turk-internet.net/portal/yazigoster.php?yaziid=51749, (accessed date; 24.11.2018).

The Telegraph Online News (2015): "Could Cyberattack on Turkey be a Russian Retaliation?", https://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html, (accessed date; 15.12.2018).

Yinanç, Barçın (2015): "Doç. Dr. Salih Bıçakcı ile Röportaj/Rusya İsterse Türkiye'yi Taş Devrine Döndürebilir", http://www.radikal.com.tr/turkiye/rusya-isterse-turkiyeyi-tas-devrine-dondurebilir-1495797/, (accessed date; 15.12.2018).

ÖZET

Devletlerin güvenliği günümüzde siber uzay temelli teknolojilere son derece bağımlıdır. 1990'lar sonrasında internetin sivilleşmesi ve ticarileşmesi ile birlikte ağ teknoloji merkezli yenilikler hayatımızın tüm alanını kapsar hale gelmişlerdir. Bu kapsamda kamu hizmetlerinin ve güvenlik faaliyetlerinin sağlandığı kritik altyapılar da önemli ölçüde sofistike yazılım programları dahilinde yönetilmeye başlanmıştır.

Bununla birlikte devletler siber uzay alanındaki teknolojilere sahip olunmaması halinde bu durumun ciddi güvenlik zafiyeti yaratacağının da farkına varmışlardır. Bu itibarla devletler siber savunma ve saldırı kapasitelerine yatırımlar yapmaya başlamışlar ve etkili siber güvenlik stratejileri geliştirmeye gayret etmişlerdir. Bu kapsamda RF'nin 2000'li yıllar sonrasında ortaya koyduğu strateji ve planlamalar ile birlikte günümüzde siber uzayı domine eden önemli bir aktör haline gelmiştir. Bu itibarla RF, günümüzde siber uzaydaki güçlü ve agresif etkinliğini dış politikada sorun yaşadığı ülkelere karşı kullanmaktan da çekinmemektedir.

RF'nin söz konusu güçlü ve agresif siber güvenlik kapasitesine sahip olma noktasındaki hedefi ise RF, temelde 1979-1989 arasında yaşanan Afganistan Savaşı esnasındaki olumsuz tecrübelere dayanmaktadır. Bu bağlamda SSCB Ordusu, bu savaş sürecinde psikolojik savaş tekniklerini uygulamada ve Afganistan'daki saha birlikleri ile Moskova'daki karargâh arasında etkili bir iletişimi sağlama noktasında yeterince başarılı olamamıştır. Bu kapsamda SSCB Ordusu'nun söz konusu zafiyetlerinin giderilmesi amacıyla Ogarkov tarafından Askeri Meselelerde Devrim (Revoluation in Military Affairs) programı gündeme alınmıştır.

Benzer şekilde 1994-1996 yıllarındaki Çeçen Savaşı esnasında RF, internet kaynaklı yeni nesil propaganda çalışmalarına karşı koymada oldukça başarısız olmuştur. Bu gelişmede RF'yi yöneten siyasi iradenin ve güvenlik bürokrasinin internet temelli teknolojilerin önemini diğer devletlerden çok daha önce kavramasına yardımcı olmuştur.

Belirtildiği şekilde RF, ulaştığı siber saldırı kapasitesi ile birlikte 2000'li yıllardan sonra uluslararası ilişkilerde sorunlar yaşadığı devletlere karşı siber imkânlarını kullanmayı dış politika stratejisinde bir yöntem olarak sıklıkla kullanmıştır. Bu itibarla RF tarafından planlandığı iddia edilen 2007 yılında Estonya'yı, 2008 yılında Gürcistan'ı ve Litvanya'yı, 2009 yılında ise Kırgızistan'ı hedef alan siber ataklar dikkat çekicidir. Benzer şekilde 14 Aralık 2015 tarihinde Türkiye'nin özellikle finans kurumlarını hedef alan "DDoS" saldırıları da RF tarafından planlandığı iddia edilebilecektir.