MODERN ÇAĞDA SİBER GÜVENLİK KAVRAMI

Seda TUNCA[1]

Özet

Bilgi iletişim teknolojilerinin hızla geliştiği 21. Yüzyılda, toplumsal yapıların ve aktörlerin her seviyesi oldukça karmaşık ve bilinmezliklerle dolu bir iklim içinde yaşamak durumundadır. İçinde yaşadığımız yüzyılın postmodern şartları içinde bulunduğumuz karışık ve bilinmezliklerle dolu dünyanın merkezindeyse kuşkusuz güvenlik kavramı yer almaktadır. Siber uzay olarak adlandırılan ve içinde bilgisayar sistemleri, online iletişim ağları ve kontrol sürecinin bulunduğu bilgi iletişim teknolojilerinin kurduğu bu devasa dünya, küresel ölçekte sosyal, ekonomik, politik ve kültürel bütünleşmenin bir parçası olarak hızla gelişmektedir. Böyle bir bütünleşmenin temelini ise bilgi oluşturmaktadır. Bilgi içinde bulunduğumuz yüzyılın en önemli üretim ve tüketim ürünüdür. Bilgiye dayalı olmayan hiçbir ürün ya da hizmet istenen kalite ve standartta sayılmamaktadır. Günümüz siber dünyasının en temel unsuru internet tabanıdır. Halihazırda kullanılan bütün bilgisayarlar, enerji hatları, telsizler, uydu sistemleri, elektrikli ve elektromanyetik her türlü cihazlar, cep telefonları, uydular, robotik sistemler insanlı ya da insansız bütün hava, kara ve deniz taşıma araçları internet tabanı üzerine kodlanmış yazılım sistemleri sayesinde çalışmaktadır. İşte bütün bu araç ve gereçler aynı zamanda siber uzay dünyasının önemli elemanları olarak değerlendirilmektedir. Bu araçların ve bir bütün halinde internet tabanının güvenliği hayati niteliktedir. Son yıllarda organize suç ve terör örgütleri faaliyetlerini planlama, eğitim, bilgiyi paylaşma ve propaganda teknikleri olarak ilgilerini siber uzaya kaydırmakta, bilgi ve iletişim teknolojilerini hedeflerine ulaşmak için kullanmaktadırlar. Devreye soktukları saldırı ve tehditler nedeniyle de siber güvenlik ve savunma faaliyetleri kişi, kurum, kuruluş ve devletler düzeyinde önemini artırmıştır.

Siber dünyanın en önemli anahtarı olan güvenlik ağı, modern hayatın olağan güvenlik kavramlarıyla bütünleşerek siber güvenlik kavramı olarak adlandırılmaya başlanmıştır. Literatürde siber güvenlik üzerine pek çok tanımlama yapılmaya çalışılmakla birlikte halihazırda bütün hatlarıyla ortaya konulmuş bir siber güvenlik kavramından söz etmek mümkün değildir. Bu durumun en temel nedeniyse siber güvenlik kavramının boyutlarının ve sınırlarının çizilememesidir. Nitekim bilgi iletişim teknolojilerinin küresel internet ağıyla bütünleşerek modern hayatın her alanına girmesi, siber güvenlik kavramının çerçevesinin çizilmesine engel olmaktadır. Bununla birlikte siber güvenlik kavramı, bilgi ve iletişim teknolojilerinin çok hızlı bir şekilde geliştiği günümüzde, kişi, kurum, uluslararası örgüt ve devletlerin en önemli gündem maddelerinden biri haline gelmiştir. Günümüzde artık önemi tartışılmaz hale gelen siber güvenlik kavramı, küresel postmodern uygarlık sürecinin gündemden düşmeyen bir konusu olacaktır.

Siber güvenlik alanında her geçen gün pek çok tehdit ortaya çıkmakla birlikte söz konusu tehditleri kategorilerine ayırmak mümkündür. Nitekim bunlardan ilki trojan, virüs, solucan olarak da adlandırılan yazılımsal tehditlerdir. İkincisiyse doğrudan insan tarafından kontrol edilen bilgisayar korsancılığı (hacker) olmalıdır. Üçüncüsü de son yıllarda giderek artan bir şekilde devreye sokulan ve hızla geliştirilen yapay zeka (artifical intelligence)'dır. Niteliği ve türü ne olursa olsun yukarıda kabaca genelleştirilen siber tehditlerin tamamının ulusal ölçekten uluslararası ölçeğe kadar artan biçimde genişlediği görülmektedir.

İşte bu çalışmada günümüz postmodern küresel dünyası içinde giderek artan siber güvenlik kavramı ele alınmıştır. Çalışma dört ana bölümden meydana gelmektedir. Birinci bölüm giriş başlığı altında konunun önemi ve günümüzde ulaştığı boyutla ilgili genel tartışmalara değinmektedir. İkinci bölüm ise siber güvenlik başlığı altında geleneksel güvenlik ve siber güvenlik kavramlarının çerçevesini ortaya koymayı amaçlamıştır. Üçüncü bölümde siber terörizm başlığı altında siber güvenlik ihlallerinin meydana getirdiği olumsuz durumlar dünyadaki belli başlı örnekleriyle ele alınmıştır. Nihayet dördüncü bölüm ise siber tehdit algısı ve siber savunma başlığı altında bugüne kadar yapılan düzenlemeler ve mücadele yöntemleri ortaya konulmuştur.

Anahtar Kelimeler: Siber, Siber Suç, Siber Güvenlik

[1] Süleyman Demirel Üniversitesi, Avrupa Birliği Çalışmaları Anabilim Dalı, Doktora Öğrencisi, sedatunca6@gmail.com

CYBER SECURITY CONCEPT IN THE MODERN AGE

Abstract

The rapid transformation of information and communication technologies in the 21st century is a complex and livable situation created by preparations. It is about the place that is sure to be full of incomprehensibility in the postmodern process that will be found. Cyberspace progresses as human beings and as part of integration with social, economic, political and competition in this world-wide global scale, in which computer systems, online communication networks and information technology in control management. The state of knowledge of such an integration. In knowledge it is the most important production and product product worldwide. Any product or service that is not based on knowledge is not considered in quality and standard. Today's cyber security is the most basic internet infrastructure. All currently used systems, radios, satellite systems, all kinds of devices, mobile phones, robotic systems, manned or all air systems, land and sea transportation internet based software systems are used. All these tools and equipment are also evaluated as numerical values. This and the internet base as a whole is of vital importance. For the sons, they use their education, knowledge and technology as organized crime and systems, space and planning techniques to achieve their goals. Cyber security and Timeshare personnel, schools and public schools branches were increased in response to attacks.

The security network, which is the most important key of the cyber world, has started to be called the concept of cyber security by integrating with the usual security concepts of modern life. Although many definitions on cyber security are tried to be made in the literature, it is not possible to talk about a cyber security concept that has already been revealed in all its lines. The main reason for this situation is the inability to draw the dimensions and boundaries of the concept of cyber security. As a matter of fact, the integration of information and communication technologies with the global internet network and its penetration into all areas of modern life prevents the framework of the concept of cyber security. However, the concept of cyber security has become one of the most important agenda items of individuals, institutions, international organizations and states today, where information and communication technologies are developing very rapidly. The concept of cyber security, whose importance has become indisputable today, will be a constant topic of the global postmodern civilization process.

Although many threats are emerging in the field of cyber security every day, it is possible to categorize these threats. As a matter of fact, the first of these are software threats, also called trojans, viruses, and worms. The second must be directly human-controlled hacking (hacker). Third, artificial intelligence (artificial intelligence), which has been increasingly introduced and rapidly developed in recent years. Regardless of their nature and type, it is seen that all of the cyber threats roughly generalized above are increasingly expanding from the national scale to the international scale.

In this study, the increasing concept of cyber security in today's postmodern global world is discussed. The study consists of four main parts. The first chapter deals with the general discussions about the importance of the subject and the extent it has reached today under the title of introduction. The second part aims to reveal the framework of traditional security and cyber security concepts under the title of cyber security. In the third chapter, under the title of cyber terrorism, the negative situations caused by cyber security violations are discussed with the main examples in the world. Finally, in the fourth chapter, under the title of cyber threat perception and cyber defense, the regulations and methods of struggle are presented.

Keywords: Cyber, Cybercrime, Cyber Security

Giriş

Teknolojinin gelişimi ile beraber internet kullanımının da yaygınlaşmıştır. İnternetin hayatımıza girmesi ile beraber hemen hemen evde bilgisayar ve telefon olması zaruri bir ihtiyaç olarak görülmesinin bir sonucudur. Bilgisayarların ve telefonların hayatımıza bu denli nüfuzu ile beraber kişisel ihtiyaçların kolaylığı ve kamu kuruluşlarındaki işleyişin hızını artırmıştır.

Teknolojik aletlerin ve internet kullanımın her ne kadar olumlu sonuçları olsa da bir o kadar olumsuz sonuçları vardır. Bu olumsuz sonuçların en başında siber güvenlik problemi gelmektedir. İnternetin kullanılmaya başlanıldığı ilk yıllarda bu sorunların ortaya çıkacağı tahmin bile edilemezken günümüzde en önemli sorun haline gelmiştir. Bilgisayar, tablet, telefon gibi taşınabilir teknolojik aletlerin hayatımıza hızla girmesi ile beraber kişisel alanda ve kamu kuruluşlarında kullanım oranı hızla artmıştır. Bu da siber güvenlik sorunlarını beraberinde getirmektedir. Kullanıcıların kişisel bilgileri, banka hesapları, kimlik bilgileri veya kamu kuruluşlarındaki bilgiler bu tehditlere açık hale gelmiştir. Ayrıca devletin gizli bilgileri, savunma sistemleri, elektrik, su ve sanayi sistemlerinin de bilgilerine bu tehditlerle ulaşmak mümkündür. Günümüz çağında artık devletler, farklı terör grupları da bu durumu kendi lehlerine çevirmişlerdir.

Siber alanda en önemli suçlardan biri olan siber terörizm de bu alanın bir parçası haline gelmiştir. Siber terörizmin genel geçer bir tanımı mevcut değildir. Günümüzde tüm devletlerce kabul görmüş terör tanımının olmaması da buna katkı sağlamıştır. Devletlerin gizli bilgileri, kamu kurum ve kuruluşların ağları, elektrik, sanayi, su gibi sistemlerine olan saldırıların tümü siber terörizmin konusu haline gelmiştir. Siber terörizmin bu denli yaygın olmasının en önemli sebebi gerçekleştiren kişi/kişileri veya devletlerin saldırıyı gizlice yapabilmeler ve açığa çıkmalarının diğer terör faaliyetlerine göre daha az oranda olmasıdır.

1.Siber Güvenlik

Siber güvenlik; internet günümüz çağında hayatımızı tamamen kuşatması ile birlikte kişiler özel hayatlarında, işyerlerinde, kamu kuruluşlarında ve devletlerarası işlerde etkin halde kullanımları söz konusu olmuştur. İnternet bilgiye ulaşmada, aktarmada kamu ve özel sektörlerdeki işleyişin daha rahat hale gelmesinde etkin rol oynamıştır. Bu kadar olumlu neticelerin yanı sıra olumsuz tehditleri de beraberinde getirmiştir. Bilgisayar ve internet kullanımının başladığı ilk yıllarda tehdit algısı söz konusu olmamıştır. 2000li yılların başlarından itibaren internetin ve teknolojik aletlerin hayatımızı ele geçirmesi ile beraber siber tehdit unsuru da ortaya çıkmıştır. (Blythe, (2013: 92-101).

Siber alanda tehditlerin ortaya çıkışı ile birlikte siber güvenlik kavramı da oluşmuştur. Kişiler veya kurumlarda kullanılan bilgisayarlarda veya diğer teknolojik aletlerde (telefon, tablet, dizüstü bilgisayar vb.) olan bilgilerin çokluğu ile birlikte bu tehdit daha da artmıştır. Kişilerin kimlik bilgileri, baka hesap bilgileri veya özel bilgilerinin bilgisayar veya diğer teknolojik aletlerde olması bu tehdide yol açacak bir durum olmuştur. Aynı zamanda kamu kuruluşlarında veya devletin gizli tuttuğu dosyalarda da bu tehditler herhangi bir açık algıladıkları takdir de kendi lehlerine durumu çevirmişlerdir. Siber güvenlik kavramı aslında gizli bilginin olduğu her durumda tehdit unsuru taşımaktadır. Kişisel veya kamu kuruluşlarındaki herhangi bir bilgisayardan internet sitelerindeki bazı reklamlara, gelen sahte maillere veya ücretsiz indirilen bazı programlara tıklayan kullanıcı farkında olmadan bilgisayarına siber bir tehdit almış olup bilgilerinin kısa sürede ellerine gelmesine mahal verecek davranışta bulunmuştur. (Coventry vd. 2014: 7-19)

Siber savaş ise, kısaca siber alanda yapılan olumlu veya olumsuz misillemelere denir. Ülkeler kendi çıkar ve menfaatlerini gözetmek için diğer ülkenin veya terör gruplarının bilişim sistemlerine verdiği zarar, kullanıma kapatmak istemesi, zarar vermesi veya durdurmak istemesi de siber savaşın bir parasıdır.(Sağıroğlu-Alkan, 2018: 21-42 (a))

"2010 yılında yayınlanan "Clatham[2] House Report" siber savaşı diğer savaşlardan ayıran en temel özellikleri aşağıdaki başlıklar altında sıralamıştır. (Cornish vd. 2010: 1)

1. Silahlı çatışmaya gerek kalmadan siyasi ve stratejik hedeflere ulaşmayı mümkün kılar.

2. Küçük ve nispeten önemsiz aktörlere orantısız güç imkânı verir.

3. Sahte IP adresleri ve yabancı sunucuların arkasında faaliyet göstererek kısa süre anonimlik sağlayabilir.

4. Konvansiyonel harpten farklı olarak kara, deniz, hava, uzay haricinde siber uzay olarak tanımlanan beşinci boyutta icra edilir.

5. Klasik harp çatışma ve baskı rejimi gibi unsurlardan sonra ortaya çıkmasına rağmen siber savaş fiziksel baskı ve çatışma ortamından uzaktır."

1.1.Siber Güvenliği Tehdit Eden Unsurlar

Siber güvenliği tehdit eden bazı unsurlar mevcuttur. Bunlar virüs, solucanlar, Truva atları, robotlar ve casus yazılımlardır.

1.1.1.Virüs

İnternette farkında olunmadan girilen bir reklam, ücretsiz program önerileri gibi görünen bir mail gibi yollarla telefon ve bilgisayar dosyalarına bulaşıp yayılan ve cihazlara zarar veren unsurlara virüs denilmektedir. Virüsler bu teknolojik aletlere bulaştıkları zaman çoğalmak için başka bir programa ihtiyaç duymaktadır. Cep telefonu ve bilgisayar gibi aletlerle bulaştıklarında dosyaları ve cihazları çalışmaz hale getirebilir, istenmeyen görüntü, yazı gibi durumları ekrana taşımaktadır. (Sağıroğlu-Alkan, 2018: 225-235 (b))

1.1.2.Solucanlar

Virüslerin aksine çoğalmak için başka bir dosya veya programa ihtiyaç duymayan, ağlar üzerinden bilgisayar veya cep telefonlarına bulaşan zararlı bir yazılım türüdür. Siber terörizm alanında zararlı yazılımlar arasında başka bir programla çoğalan neredeyse tek yazılım türüdür.(Yıldız, 2014: 42-44)

1.1.3.Truva Atları

Truva atları bilgisayar ve cep telefonlarına bulaştıklarında normal bir dosya niteliğinde görülmekte fakat arka planda dosya açabilmekte, girilen cep telefonu veya bilgisayara uzaktan erişim sağlayabilmekte olan zararlı bir yazılım türüdür. Normal bir program gibi görünen, fakat kötü amaçlı kodlar barındıran programlar arasındadır. Truva atlarını bilgisayar ve cep telefonlarında fark etmek oldukça zordur. Fakat bulaştığı andan itibaren sistemi ve işleyişi yavaşlattığı için fark edilmektedirler. Solucanlar ve virüsler den ayıran özellik ise, farklı dosyalara bulaşıp çoğalamamaktadırlar. (Yıldız, 2014: 42-44)

1.1.4.Robotlar

Bilişim dünyasında robot olarak adlandırılan fakat bir diğer adıyla bot olarak tanımlanan bir kavramdır. Bir dizi bot oluşumundan kaynaklanan ve ağlarla bilgisayar ve diğer teknolojik aletlere bulaşan zararlı yazılımlardır. Botlar, bulaşacakları bilgisayar ve diğer teknolojik aletlerin en güçsüzlerini seçerek alışmaz hale getirmektedirler (Jang-Jaccard vd, 2014: 973-993)

1.1.5.Casus Yazılımlar

Bilgisayar kullanıcılarının kişisel vi gizli bilgilerini, kamu kurumlarının veya şirket bilgilerinin erişimi ve diğer üçüncü kişilere dağıtımı için ortaya çıkan zararlı bir yazılım türüdür. Özellikle devletlerarasında veya siyasi liderlerin gizli bilgilerinin üçüncü kişilere aktarımı için kullanılan zararlı bir yazılım türüdür. Casus yazılımlar web sitelerine ya da ücretsiz paylaşılan yazılımlara gömülerek yayılmaktadırlar *"CoolWebSearch", "Cydoor" , "BlazeFind" ve "Gator"* casus yazılımlara örnek gösterilmektedir. (Sağıroğlu- Alkan, 2018; 21-42)

2.Siber Terörizm

Modern dönemde internetin hayatımıza girmesiyle birlikte bilgisayar ve diğer teknolojik (cep telefonu, dizüstü bilgisayarı, vb.) aletlerinde gelişimi aynı doğrultuda artış göstermiştir. Bu artış sayesinde kişisel kullanım, kamu kurumlarında ve özel sektörlerde bilgisayarlar yerini hızla almış ve işleyişi değiştirmiştir. Bilgisayar kullanımının yaygınlaştığı kişiler ve kurumlar gizli bilgileri, kimlik bilgilerini, banka hesap bilgileri vb. açık bir şekilde ortaya koymaktadır. Bu durumda bilgilerin açığa çıkması, özel hayatın ihlali, üçüncü kişilerce kullanım gibi durumları da beraberinde getirmiştir. Teknolojinin geliştiği ilk yıllarda bu tür olumsuz eylemlere karşı bir savunma sistemine ihtiyaç duyulmamıştır. Fakat günümüzde bu tür eylemler çok fazla yaşanmaktadır. Modern çağın getirdiği olumsuz neticeler arasına siber terörizm kavramı da girmektedir. Siber terörizm, diğer terör eylemlerine göre teröristlere askeri, fiziksel, psikolojik eğitim vermeden, can ve mal kaybına uğramadan bilgisayar ağları üzerinden gerçekleştirilen eylemlerdir. Siber terörizm maliyet açısından da terör gruplarını etkilemediği için revaçta olan eylemler arasındadır. Siber terörizmin amacı; devletleri baskı altına almak, otoriteyi sarsmak, yıkıcı faaliyetlerde bulunmak, devletlerin ve devlet adamlarının gizli bilgilerini ortaya çıkarmak ve kendi çıkarları doğrultusunda kullanmak, gerçekleştirilen ülkede elektrik, su, ulaşım gibi sistemlerini ele geçirip işleyişi durdurmak gibi eylemlerin tümü siber terörizm faaliyetleri arasındadır. (Gürkaynak-İren, 2011; 266-267)

2.1. Dünyada Siber Saldırı Örnekleri

Soğuk savaş sonrasında Rusya ve ABD artık strateji değiştirmiş ve saldırıları artık siber alana taşımıştır. 1982 yılından Moskova, Kanada dan aldığı doğalgaz şirketinin boru hatlarının kontrolü için yazılımı almaya başlamıştır. Bunun üzerine durumu fark eden ABD çalınan yazılımın içerisine virüs yüklemiş ve boru hatlarındaki doğalgaz akışının dengesini bozmuştur. Dengesi bozulan ve normalinden daha fazla akış sağlandığı için bir süre sonra Rusya sınırlarında bir patlama gerçekleşmiştir. Bu durum da siber savaşın başladığı ilk olay olarak tarihe geçmiştir.(http://www.ckk.com.tr/ders/communication.pdf, 01.06.2019)

Dünyada siber saldırılara bir diğer örnek ise, 1992 yılında ABD ile Irak arasında yaşanmıştır. Savaş başlamadan önce ABD, Irak'ın tüm iletişim sistemlerini ele geçirmiş ve bu durumu kendi çıkarları doğrultusunda yönlendirmiştir. 2003 yılına gelindiği zaman Irak'ı işgal etmeyi planlayan ABD, Irak Savunma Bakanlığının veri tabanını işgal etmiş ve çalışanlarına bilgisayar ekranları üzerinde bir mesaj göndermiştir. Mesajda, " *yakın bir zamanda Irak'ı işgal edebiliriz, sizlere zarar vermek istemiyoruz, savaş başladığında evlerine gidin "*çağrısını vermiştir. Mesajı dikkate alan çalışanlar ve hatta askerler yerlerini terk etmişlerdir. Yerlerini terk eden Irak askerlerinin tankları kolaylıkla imha edilmiştir. (http://www.ckk.com.tr/ders/communication.pdf, 01.06.2019)

Yukarıda verilen örneklere bakılacak olursak teknolojinin ve internetin hayatımıza girmesiyle savaş stratejilerinde de değişimler yaşanmıştır.

2.2.Siber Güvenlik Unsurları Ve Önerileri

Siber saldırıları azalması için devletler tedbir almaktadır. Bu tedbirler uluslararası alanda da mevcuttur. Fakat siber alanda da olduğu gibi terör kavramının da tüm devlerce kabul görmüş bir tanımı mevcut değildir. Bu sebeple bu konu ile ilgili devletlerce çok az sayıda antlaşmalar imzalanmıştır. Ortak bir çatı altında toplanamayan ülkeler kendi tedbirlerini kendileri almaktadır. Çünkü devletler birbirlerine saldırıları BM'ye barışa ihanet etmemek için silahlı bir saldırı yapmaktansa, siber alanda savaş açmaktadır. Devletler diğer devlerin gizli bilgilerini, siyasi liderlerin konuşmalarını, devletlerin elektrik, su, doğalgaz gibi hayati kaynakların ağlarına müdahale etmek için bu alana başvurmaları kaçınılmaz hale gelmiştir.

Sonuç

Siber güvenlik, günümüz çağdaş toplumlarında internetin hayatımızın merkezine oturması ile ortaya çıkan bir kavramdır. İnternetin gelişme ile cep telefonu ve bilgisayar gibi teknolojik aletlerin gelişimi de hızla artmıştır. Bu durumun olumlu yönleri ve olumsuz yönleri de vardır. Hayatımızı kolaylaştırması, kurumsal ve kişisel işleyişin hızlanması gibi olumlu yönleri vardır. Kullanılan bu cihazlara kişisel ve kurumsal bilgiler de yüklenmiş ve bu durumu kendi çıkarları için kullanacak kişi/kişilerin ellerine geçmesi de olumsuz bir yönü olarak değerlendirilmektedir.

İnternet ve teknolojiyi terör amaçlı ve devletlerin gizli bilgilerinin ortaya çıkması için, siyasi liderlerin gizli yazışma ve bilgilerinin açığa çıkması için kullanan kişi veya kişiler mevcuttur. Siber terörizmin, terörün tanımı gibi tüm devletlerce kabul görmüş bir tanımının mevcut olmaması da, siber terörizme olan çözümde sorunların ortaya çıkmasına olumsuz katkıda bulunmuştur.

Siber alan, siber güvenlik ve siber terörizm kavramları günümüzde en revaçta olan akademik konudur. Son dönemlerde yapılan araştırmalar incelenecek olunursa, siber terörizm konusu dünyada ve ülkemizden önemli sorun olduğu için son dönemlerde üzerinde çok durulmuştur.

İnternetin ve bilgisayarın hayatımıza girmesi, hemen hemen her evde bilgisayarın olması siber terörizmi hızlandırmıştır. Bu sebeple artık siber alana müdahale ve tedbirler alınmaktadır. Tedbirlerin yetersizliği ise, ülkelerin ortak bir çatı altında toplanamamasıdır. Kavramsal olarak ortak bir kanıya varamayan ülkeler, siber terörizme çözüm konusunda yetersiz kalmışlardır.

Kaynakça

Blythe, J., (2013). Cyber Security In The Workplace: Understanding and Promoting Behaviour Change. Proceedings Of Chıtaly 2013 Doctoral Consortium,

Coventry L., Briggs, P., Blythe, J., Tran, M. (2014). Using Behavioural İnsights To İmprove The Public's Use Of Cyber Security Best Practices. Report.

Gürkaynak M., İren A.A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt.16, Sayı.2.

Jang-Jaccard, J., Nepal, S. (2014). A Survey Of Emerging Threats In Cybersecurity,' Journal Of Computer and System Sciences, Cilt 5, Sayı:80.

Cornish, P., Livingstone, D., Clemente, D., Yorke, C., (2010). On Cyber Warfare A Clatham House Report.

Sağıroğlu Ş., Alkan, M., (2018a). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınevi, Ankara.

Sağıroğlu Ş., Alkan, M., (2018b). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınevi, Ankara,

Yıldız, M. (2014). Siber Sular ve Kurum Güvenliği, Denizcilik Uzmanlık Tezi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

http://www.ckk.com.tr/ders/communication.pdf, (01.06.2019).

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi International Journal of Multidisciplinary Studies and Innovative Technologies, Cilt:1, Sayı: 1.

Şenol, M. (2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, Sayı:2.

Sertelik A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak, Medeniyet Araştırmaları Dergisi, Cilt: 2 Sayı: 3.

Şeker, E. (2017). Savunma Tatbikatları: Planlama, Uygulama ve Değerlendirme", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, Sayı:2.