SİBER OLAYLAR EKSENİNDE SİBER GÜVENLİĞİ ANLAMAK

Aşır SERTÇELİK*

Öz: Siber uzay teknoloji ile birlikte ortaya çıkmıştır. İnsanların siber uzay ile olan ilişkisi arttıkça siber uzay da güvenlik meselesi de yeni bir boyut kazanmaktadır. Gerçekleşen bir takım siber olayları anlamamız siber güvenliği anlamamız açısından temel teşkil etmektedir. Siber güvenlik, içerik itibarı ile bilgisayar sistemleri ve genel olarak teknoloji ile iç içe geçmiş olduğundan ve teknik boyutları birçok farklı çalışmanın konusunu teşkil ettiğinden siber güvenliğin teknik ayrıntıları ele alınmamıştır. Sınırları belli olmayan siber uzayda güvenlik konusu ise birey, devlet, uluslararası ve hatta küresel düzeyde bir ihtiyaçtır. Çalışmada bu ihtiyaca dikkat çekmek amaçlanmıştır.

Anahtar Kelimeler: Güvenlik, Siber Güvenlik, Siber Olaylar.

UNDERSTANDING CYBER SECURITY ON AXIS OF THE CYBER EVENTS

Abstract: Cyberspace has emerged with technology. As the relation increase between people and cyber space, The issue of security in cyberspace also gains a new dimension. A series of cyber events are the basis for understanding cyber security. Cyber security has been intertwined with computer systems and technology in general. Technical aspects of cyber security for constituting the subject of many different studies have not been addressed. Security in cyberspace without boundary is a necessity of individual, state, international, and even global. It is aimed to draw attention to this need in the study.

Keywords: Security, Cyber Security, Cyber Incidents

I. Giriş

İçinde bulunduğumuz çağ, bilginin değerinin her geçen gün artması ile birlikte, bilgi çağı olarak adlandırılmaktadır. Sürekli bir gelişim içerisinde olan internet ve bilgisayar teknolojileri, ihtiyacımız olan bilgiye daha kolay ve hızlı bir şekilde ulaşmamıza imkân sağlamaktadır. Biz interneti dijital dünyanın bir kısaltması olarak kullanırken; bu bilgisayarların arkasındaki insanları ve onların bağlantılarının toplumlarını nasıl değiştirdiğini kapsayan bir siber uzay var. (Singer & Friedman, 2014, s. 14)

Siber; oluşturulan, depolanan ve paylaşılan sayısallaştırılmış verilerden oluşan bir bilgi ortamıdır. (Singer & Friedman, 2014, s. 13) Siber uzay ise ABD Savunma Bakanlığı'nca "internetin bulunduğu, telekomünikasyon ağlarını ve bilgisayar sistemlerini de kapsayan, birbirine bağlı bilgi teknolojisi altyapılarının olduğu küresel bir alan" olarak tanımlanırken, ayrıca "insanların, telekomünikasyon sistemleri ve bilgisayarlar aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan, birbirine bağlı olma durumu" şeklinde de tanımlanmaktadır. (Habertobb, s. 13) Siber uzay kavramı ilk defa 1974 yılında

* Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı Tezli Yüksek Lisans Öğrencisi. e-mail: asirsertcelik@gmail.com

Geliş Tarihi: 01 Aralık 2017
Date of Received: *01 December 2017*
Kabul Tarihi: 09 Şubat 2018
Date of Accepted: *09 February 2018*

William Gibson tarafından kullanılmıştır. (Karakuzu, 2015, s. 72) Siber uzay interneti kapsayan ancak salt internetten ibaret olmayan bir sistem olarak kabul edilmektedir. (Özçoban, 2014, s. 51) Siber uzayda net sınırlar yoktur.

Fiziksel alanın yerini siber uzaya bırakmaya başlaması ile beraber zamana ve mekana bağlılık önemli ölçüde azalmış, hiyerarşik yapının yerini demokratik yapı ve doğallığın yerini teknoloji almaya başlamıştır. Kısacası günümüzde yaşamın birçok alanı Bilgi İletişim Teknolojilerine bağımlı hale gelmiştir ve bu bağımlılık da giderek artmaya devam edecektir. (Ünver & Canbay, 2010, s. 95) Bu gelişmeler bir taraftan insanoğlunun yaşamını önemli ölçüde kolaylaştırıp, rahatlaştırırken diğer taraftan da "siber güvenlik" başta olmak üzere bir takım problemlerin ortaya çıkmasına yol açmaktadır. İnternet kullanımında güvenlik, internetin tasarımından daha sonra ortaya çıkmış olan bir olgudur. İnsanoğlu için çok büyük faydalar sağlayan bu gelişmelerin art niyetli bazı kişiler tarafından suistimal edilmesi, siber ortamın saldırı, tehdit, mala ve hatta cana zarar vermek amacı ile kullanılması ve siber saldırılar sebebi ile kişilerin ve ülkelerin gördüğü zararların büyük boyutlara ulaşması güvenlik algısında ve anlayışında bir takım değişikliklere yol açmış ve siber güvenlik konusu bireylerin, kurumların, ülkelerin ve uluslararası kuruluşların gündeminin en önemli gündem konularında biri haline gelmiştir. (Ünver & Canbay, 2010, s. 94)

Siber Uzay ile birlikte güvenlik tanımı da değişime uğramıştır. Devlet merkezli, askeri tehdit odaklı bir bakış açısı içinde yorumlanan geleneksel güvenlik anlayışı, büyük ölçüde suni tehditler üzerinden güvenlik gündemini belirlemiştir. (Karabulut, 2009, s. 2) Güvenlik artık sadece devletlerin fiziksel olarak hayatta kalmalarını değil aynı zamanda insanların hayat tarzları, değerleri, toplumsal ilişkileri vs. olarak korunmasını da içermektedir. (Karabulut, 2009, s. 2) Siber güvenlik, "siber hayatın güvenliğinin (gizlilik, bütünlük ve erişilebilirlik) sağlanması amacıyla gerçekleştirilen faaliyetlerin tümü (Uçar, 2011, s. 7)" olarak tanımlanmaktadır. Gizlilik, bilişim sistem ve verilerine sadece yetkili sistemler veya kişiler tarafından erişilebilmesini ifade eder. Bütünlük, bilgi ve bilişim sistemlerinin ve sadece yetkili sistemler veya kişiler tarafından değiştirilebilmesini ifade eder. Erişilebilirlik ise, yetkili kişilerin ihtiyaç duyulan zamanda ve ihtiyaç duyulan kalitede bilgiye ve bilişim sistemlerine erişebilmesini ifade etmektedir. (Kara, 2013, s. 4-5) Gizlilik, bütünlük ve/veya erişilebilirlik ihlal edildiği zaman bu bir tehdittir ve siber güvenlik konusuna girer. Siber Güvenlik, siber uzaydan gelebilecek tehdit ve saldırılara karşı kurum, kuruluş ve bireylerin varlıklarını korumak amacı ile kullanılan risk yönetimi yaklaşımları, güvenlik kavramları, politikalar, eğitimler, kılavuzlar, güvenlik teminatları, faaliyetler, uygulamalar, araçlar ve teknolojilerden oluşmaktadır. (Siber Güvenlik)

Güvenlik kavramı ilk insanla birlikte hayatımıza girmiş ve günümüze gelene kadar çeşitli evrelerden geçmiştir. Güvenlik sözlük anlamı içinde; "toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet (Türk Dil Kurumu)" olarak tanımlanmaktadır. Arnold Wolfers bu tanımlamayı iki farklı bileşene bölerek bir güvenlik tanımlamasına ulaşmaya çalışmıştır. Wolfers'a göre güvenlik; objektif anlamda eldeki değerlere yönelik bir tehdidin olmaması ve subjektif anlamda ise bu değerlere yönelik bir saldırı olacağı korkusu taşımamaktır. (Karabulut, 2009, s.

3) Yeni tehditlerin ortaya çıkmasıyla beraber güvenliğin genişlemesi ve derinleşmesi de bir zorunluluk haline geldi. Ekonomi güvenliği, bilişim güvenliği, bilgi güvenliği, birey güvenliği, doğal kaynakların güvenliği vs. gibi birçok güvelik alanı ortaya çıktı. Siber güvenlik ise aslında tüm bu yeni güvenlik alanlarının kesişim noktasında yer almaktadır. (Boyraz) Sıradan bir siber saldırı birey ve bilgi güvenliğini doğrudan etkileyebilmekteyken, kapsamlı bir siber saldırı ekonomi ve çevre güvenliğini, toplumsal hatta küresel güvenliği doğrudan etkileyebilmektedir.

Küreselleşme sürecinin ivme kazanmasına paralel olarak dünyada hemen her alanda değişim ve dönüşümler yaşanmaktadır. Bu alanlardan biriside güvenliktir. Siber ortamda bilgilere ve bilişim sistemlerine yönelik kötü niyetli hareketlerin ve saldırıların başlaması ve bunların artarak devam etmesi 'Siber Güvenlik-Savunma' kavramlarını, karşı tarafın bilgilerine ve bilgi sistemlerine zarar verme veya olumsuz etkileme istek ve ihtiyaçları ise 'Siber Saldırı-Taarruz' kavramlarını ortaya çıkarmıştır. (Şenol, 2016, s. 10) Bilgi ve iletişim teknolojilerindeki gelişmelerle siber ortamın sağladığı imkân ve kolaylıklar yaşamı her geçen gün kendisine daha bağımlı hale getirirken, bu ortamın tehdit, saldırı, cana ve mala zarar verme vb. amaçlarla kullanılması sonucunda kişilerin, toplumların ve ülkelerin uğradığı büyük zararlar güvenlik anlayışında büyük değişikliklere yol açmıştır. (Şenol, 2016, s. 11)

Bilgi iletişim teknolojileri konularında çalışmalar yürütmekte olan Birleşmiş Milletler'in haberleşme, bilgi ve iletişim teknolojileri alanındaki yetkili organı Uluslararası Telekomünikasyon Birliği'dir. Özel sektör ve kamu kuruluşlarına bilgi iletişim teknolojileri alanında hizmetler sunmaktadır. Başlıca görevleri arasında uydu yörüngelerinin tahsisi konusunda uluslararası işbirliğini sağlamak, radyo spektrumunun küresel ölçekte kullanımını düzenlemek, farklı haberleşme sistemleri arasında bağlantılar sağlanmasına izin veren dünya standartlarını oluşturmak gibi görevleri bulunmaktadır. Tüm bunların yanı sıra, siber güvenliğin sağlanması gibi güncel konularda da çalışmalar yapmaktadır. Türkiye'nin de dahil olduğu 191 devlet üyesi ve 700'den fazla sektör temsilcisini bünyesinde barındırmaktadır. Dünyada siber güvenlik konusunda etkin rol oynayan önemli bir uluslararası kurumdur. UTB tarafından yapılan tanımda siber güvenlik, "siber uzayda, kullanıcılar ve organizasyonların varlıklarını korumak amacı ile kullanılan politikalar, risk yönetimi yaklaşımları, araçlar, güvenlik kavramları, güvenlik önlemleri, uygulamalar, kurallar, eylemler, eğitimler ve teknolojilerin bütünü" olarak ifade edilmiştir. (Çeliktaş, 2016, s. 18-19) Başka bir tanımda ise siber güvenlik, bir devletin kendisini ve kurumlarını casusluk, tehdit, sabotaj, dolandırıcılık ve suçtan koruyabilme, hırsızlığı ve diğer yıkıcı e-etkileşimleri ve e-işlemleri tanımlayabilme kabiliyetini ifade eder. (Choucri, 2012, s. 39)

Siber güvenlik, donanım güvenliği, fiziksel güvenlik ve bilgi güvenliğinden oluşmaktadır. İnternetin temel felsefe bilgi paylaşımı olduğu için güvenlikte de en hassas olan bilgi güvenliği konusudur. Yapılan araştırmalar, bilgi güvenliği olaylarının %14'ünün satış noktası ihlallerinden, %22'sinin siber casusluktan ve %35'inin web saldırılarından olduğunu gösterdi. (Habertobb, s. 15)

Siber güvenlik 1990'lardan bu yana ulusal güvenlik için öne çıkmış bir konudur. İki kutuplu uluslararası sistemin yapısı etkisini kaybetmesi ile birlikte

uluslararası güvenlik sadece askeri kökenli olmaktan çıkıp ekonomiden enerjiye, iklim değişiminden siber alana kadar yeni tehditler tartışılmaya başlanmıştır. (Bıçakcı, 2012, s. 206) Her devletin kendi içerisine bir takım siber güvenlik önlemleri vardır. Siber tehditler yaşandıkça devlet, kurum ve bireylerin tedbirlerini artırma zorunluluğu doğmuştur. Özellikle bu konuda devletler bazında yasal düzenlemeler, tedbirler ve siber olaylara müdahale birimleri kurulmaya başlanmıştır. Kritik altyapıların günümüzde tamamen bilgi iletişim teknolojilerine bağımlı hale gelmesi hem bireyler hem ülkeler hem de uluslararası toplum açısından hayati bir önem arz etmektedir. (Ünver & Canbay, 2010) Bu konuda yapılan çalışmalar siber güvenlik çalışmalarının ulusal strateji ve politika geliştirilmesi, kurumsal yapılanmanın belirlenmesi, yasal çerçevenin oluşturulması, teknik tedbirlerin geliştirilmesi, ulusal koordinasyon ve işbirliğinin sağlanması, farkındalığın artırılması, kapasitenin geliştirilmesi, uluslar arası uyum ve işbirliğinin sağlanması olarak sekiz önemli unsuru olduğunu ortaya koymaktadır. (Ünver & Canbay, 2010, s. 99)

İnternet, fiziksel olarak sınırlandırılamayan ve ulusal sınırları aşan yapısı sayesinde Uluslararası İlişkiler'in alanına girmektedir. (Öğün & Kaya, s. 148) Siber dünyanın birçok özelliği de çağdaş uluslararası ilişkiler teorisini, politikasını ve uygulamasını yeniden şekillendirmektedir. (Choucri, 2012, s. 3) Siber Uzay'da bir aktörün faaliyetleri, diğer aktörlerin egemenliğini, istikrarını veya güvenliğini tehdit ettiğinde, Siber Uzay uluslararası ilişkilerde kritik bir alan haline gelmeye başlamıştır. (Choucri, 2012, s. 5) Yakın zamana kadar Siber Uzay'a ilişkin meseleler "low politics" bir mesele olarak ele alınırdı. Ama artık Siber Uzay'ın ulusal güvenlik ve alışılagelmiş uluslararası düzenin bozulması açısından potansiyel bir tehdit oluşturan bir güvenlik açığı kaynağı olduğu anlaşılmıştır. (Choucri, 2012, s. 3) Önemli siber güvenlik olayları siber güvenliğin ne kadar önemli bir mesele olduğu konusunda ikna edici bir rol oynamış ve siber uzay ile ilgili sorunların gitgide "high politics" bir mesele olarak ele alınmasını sağlamıştır.

Siber tehditlerin boyutlarının devletlerarası krizlere yol açacak kadar büyümesi ve devletlerin siber alanı bir hâkimiyet unsuru olarak görmeye başlamaları gibi durumlar siber alanı daha çok güvenliksizleştirmektedir. Siber güvenliğin uluslararası güvenlikle ilişkili olduğunu göz önüne alırsak, siber güvenlik sorunun uluslararası ilişkilerdeki anarşiyi artıracağını da kabul etmemiz gerekir.

Siber güvenlik konusunda siber suçlara karşı uluslararası düzeydeki ilk sözleşme Avrupa Konseyi tarafından hazırlanan Siber Suç Sözleşmesi'dir. Sözleşmeyi 39 Avrupa Konseyi üyesi, ABD, Kanada, Japonya ve Güney Afrika olmak üzere toplam 43 ülkenin imzaladığı biliniyor. Türkiye ise 10 kasım 2010 tarihinde Dışişleri Bakanlığı düzeyinde bu belgeyi imzaladı. (habertobb, s. 17) Sözleşme, ulusal ceza hukukunu uyumlaştırmayı, suçların soruşturulması ve kovuşturulması için ulusal ceza usul hukuku yetkisini geliştirmeyi ve uluslararası işbirliği için etkili mekanizmalar kurmayı amaçlıyor. (Choucri, 2012, s. 168) Fakat siber suç, siber güvenlik alanındaki mevcut güvenlik eksikliğinin yalnızca bir parçasıdır. (Knake, 2010, s. 21) Siber güvenlik kavramının yeri ve öneminin her geçen gün arttığı düşünülürse, dünya barış ve güvenliğinin sağlanabilmesi için uluslararası hukuk kuralları içerisindeki yerinin netleştirilmesi önemli bir meseledir. Bütün bunların yanında, Küresel

çapta Birleşmiş Milletler tarafından bu konuda kabul edilmiş bir anlaşma olmadığından, dünya çapında az ve çok üzerinde uzlaşılan ve kabul edilen bir siber güvenlik tanımı da yoktur. (Akyeşilmen, 2016) Küresel çapta üzerinde anlaşılan bir siber güvenlik tanımı olmadığı için uluslararası siber güvenlik siyaseti oluşturmakta zordur. Uluslararası siber güvenlik siyasetinin olmayışı her devletin kendi başına buyruk bir siber güvenlik siyaseti oluşturmasında itici bir rol oynamaktadır.

Zaman içerisinde, bilginin, ticaretin ve ekonomik sistemlerin internet ile bütünleşik hale gelmeleri ve siber alanda yaşanan gelişmelerin sistemlere yetkisiz girişe, bilgi hırsızlığına ve hatta fiziksel zararlar vermeye kadar imkân tanıması siber alanda güvenliği büyük bir sorun haline dönüştürmüştür. (Güngör & Güney, 2017, s. 138) Siber suçların her yıl dünya ekonomisine verdiği zarar yaklaşık 1 trilyon dolar civarındadır. (Knake, 2010, s. 5) Sadece bu zarar bile göz önüne alındığında uluslararası alanda siber güvenlik konusunda atılacak adımların ne kadar gerekli olduğu tahmin edilebilir.

Dünyanın gelecekte nerede olacağına ilişkin bir ankette Foreign Policy dergisi, siber alanı "tek ve en büyük gelişmekte olan tehdit" olarak nitelendirirken, Boston Globe geleceğin burada olduğunu iddia etmiştir. (Singer & Friedman, 2014, s. 3) ABD eski Başkanı Barack Obama ise "siber güvenlik risklerinin 21. yüzyılın en ciddi ekonomik ve ulusal güvenlik zorluklarının bir kısmını teşkil ettiğini" beyan etmiştir. (Singer & Friedman, 2014, s. 2)

II. Siber Güvenlik Olayları

Hiçbir zaman tam bir güvenlik yoktur, çok düşük bir ihtimalde olsa güvenlik açıkları hep vardır. Siber güvenlik içerisinde yönelik hem doğal hem beşeri olaylar vardır. Üzerinde durulan ise daha çok beşeri olaylardır. Siber uzayda, güvenlik alanındaki mücadele farenin hep bir adım önde olduğu kedi-fare mücadelesine benzetilmektedir. (Özçoban, 2014, s. 87) Siber olaylar, siber güvenliğin ne kadar önemli bir mesele olduğu konusunda ikna edici bir rol oynamıştır. Siber güvenliği etkin bir şekilde sağlamak için, siber olayları ve çoğunlukla da siber tehditleri anlamak gerekir. Siber güvenlik alanında şuan için önemli bir tarihsel birikim ve gelişim yoktur. Fakat siber meselelerin sebep olduğu siber güvenlik algısının gelişimi söz konusudur.

Siber güvenlik konusu ile ilişkili önemli siber olaylara bakacak olursak eğer;

Haberleşmenin/Bilginin Gizliliği ve Şifreleme Üzerine: Şifrelemedeki temel mantık bilgi ve iletişimin güvenliğini sağlamak olmuştur. Bu amaçla tarih içerisinde bir takım girişimler ortaya koyulmuştur. Bilinen ilk sistematik şifreleme yöntemi olan Sezar şifresi, Antik Romalılar tarafından M.Ö. 1. yy.'da kullanılmıştır. Bu yöntemde temel fikir kullanılan yazışma dilindeki harflerin başka harflerle değiştirilmesi olmuştur. Sezar şifresinin ardından 7. yy.'da El Kindi tarafından bir şifre kırma yöntemi geliştirilmiştir. El Kindi bu tekniği Risalah fi Istikhraj al-Mu'amma (şifrelenmiş mesajları kırma) kitabında ortaya koymuştur. (Siber Güvenlik Olayları)

15.yy'da Leon Battista Alberti tarafından sıklık analizine dayalı yöntemin geliştirilmesi ile Çok Alfabeli Şifreleme yöntemi ortaya koyulmuştur. Leon Battista Alberti'nin bu tekniği ortaya koyması batı kriptografisinin babası olarak anılmasına sebep olmuştur. Giovan Battista Bellaso tarafından 16. yy'da

yılında "La cifra del. Sig. Giovan Battista Bellaso" adlı kitabında Vigenère Şifrelemesi yöntemi ortaya koyulmuştur. Bilinen ilk anahtara dayalı şifreleme yöntemi olmuştur. Bu yöntem temelde olarak Sezar şifrelemesi ya da çok alfabeli şifrelemeye benzemektedir. Fakat farklılık olarak kolaylıkla değiştirilebilen bir anahtar ifadenin kullanılmasına olanak tanımıştır. İlk kullanılan anahtarlar ise genelde her iki tarafın bildiği, kısa kelimeler ya da ifadelerden oluşmuştur. (Siber Güvenlik Olayları)

Friedrich Kasiski, Edgar Allan Po ve Charles Babbage gibi araştırmacılar, çok alfabeli kripto sistemlerin kırılması üzerine 19.yy'da sistematik yaklaşımları ortaya koymuşlardır. Auguste Kerckhoffs ise askeri şifreleme üzerine 19.yy'da iki makale yazmıştır. Makalelerinde, gizli anahtar kullanımına dayalı şifreleme yönteminin en temel ilkelerini ortaya koymuştur. Makaleye göre kullanılan bir kripto sisteminde gizlilik, şifreleme mekanizmasının veya algoritmanın gizliliğine dayandırılmamıştır Tam aksine, gizlilik anahtarın gizliliğine dayandırılmıştır. Kripto sistemi düşman eline geçmesi durumunda tüm sistemin güvenliği ortadan kalkacağı için güvenlik bir anahtarın gizliliğine dayandırılmıştır. Bir anahtarın gizliliği ortadan kalkarsa, yenisi ile tekrardan kripto işlemi yapılabilmesini esas almıştır. (Siber Güvenlik Olayları)

Birinci Dünya Savaşı sırasında İngiliz deniz kuvvetlerinin kurmuş olduğu Room 40 kod adlı birim Almanların mesaj şifreleme tekniklerinin kırılması için bilinen ilk resmi şifre kırma birimi olmuştur. Bu birimin çalışmaları İngiliz ve Alman donanmaları arasındaki deniz savaşlarında oldukça etkin olmuştur. (Siber Güvenlik Olayları)

Gilbert Vernam 1917 yılında geliştirilen bir tele-yazıcı açık metni önceden belirlenen bir anahtar kullanarak şifreleyebilmiştir. Şifre makinesi olarak bilinen bu tasarım elektromekanik sistemlerin geliştirilip ve tek kullanımlık şifrelerin ortaya çıkmasına yol açmıştır. Bu şifrelerin kırılması pek mümkün değildir. (Siber Güvenlik Olayları)

Marian Rejewski 1932 yılında istatistiksel kripto kırma yöntemlerini kullanarak Alman ordusuna ait Enigma sistemini kırmayı başarmıştır. Bu olay kriptolojinin 1000 yıllık en büyük olayı olarak nitelendirilmiştir. (Siber Güvenlik Olayları)

İkinci Dünya Savaşı'nın ardından şifreleme, tamamen anahtar kullanımına dayalı olarak geliştirilmiş ve geçmişteki diğer yöntemler terk edilmiştir. (Siber Güvenlik Olayları)

1949 yılında Claude Shannon "Kriptografinin bir matematiksel kuramı" adlı makalesinde şifre kırılabilirliği ve mükemmel şifrelemeyi matematiksel/kavramsal olarak tanımlamıştır.Bu olay çoğunluk tarafından kriptografinin, sanattan bilime geçişi olarak tanımlanmıştır. (Siber Güvenlik Olayları)

1975 yılında IBM'deki bir grup Amerikan Ulusal Standartlar Bürosu'nun daveti üzerine, gizli anahtar şifrelemesine dayalı bir yaklaşım olan DES'i (Data Encryption Standard) yayımlanmıştır. DES bir ulusal kurum tarafından kamuya ilan edilen ilk şifreleme standardı olmuştur. 2001 yılında ise DES standardı, AES (Advanced Encryption Standard) standardı ile değiştirilmiştir. Bunun temel nedeni ise DES'in 56 bitlik anahtarının makul sürelerde kırılabilmiş olması olmuştur. Elektronic Frontier Vakfı'na üye bir

grup 1997 yılında 56 saatte DES şifresini kırmayı başarmıştır (Siber Güvenlik Olayları)

1976 yılında Martin Hellman ve Whitfield Diffie tarafından "Kriptografide Yeni Yönler" adlı makale ortaya koyulmuştur. Bu makale kripto sistemlerinin çalışmasını kökten değiştirmiştir. Kriptografi'de en temel sorunlarından biri olan anahtar dağıtımı sorununu, anahtar değişimi yöntemiyle çözüme kavuşturulmuştur. Bu gelişme, asimetrik şifreleme algoritmalarının geliştirilmesinde önemli rol oynamıştır. (Siber Güvenlik Olayları)

Siber Teknoloji Kullanılarak Gerçekleştirilen İlk Siber Saldırı (1982): Tarihte siber teknolojinin verdiği imkanlar çerçevesinde gerçekleştirilen ve ilk siber saldırı olduğu düşünülen saldırı 1982 yılında Sibirya'da yaşanan patlama olmuştur. Saldırı, Sibirya doğal gaz boru hattında patlamaya sebep olmuştur. Sovyetler Birliği ve ABD arasında casusluk faaliyetlerinin yürütüldüğü Soğuk Savaş döneminde meydana gelmiştir. 1982 yılında Rusya Kanada'da bir şirketten doğal gaz boru hatlarını kontrol etmek için kullanılan bir yazılımı çalmıştır. Rusların Kanada'dan gizlice çaldık zannettikleri aslında CIA tuzağı ile tuzaklanmış virüslü bir yazılım olmuştur. Amerikalılar, yazılım içerisine Truva atı virüsü yüklemiştir. Amerikalılar, Rusların yazılımı çalmaya başladıklarını fark etmiştir. Fakat operasyona engel olmak yerine yazılımın içine virüs yerleştirmeyi tercih etmiştir. Rusların çalmış olduğu yazılım bir süre sonra bozulmuştur. Virüs boru hatlarındaki akışı anormal seviyelere çıkartarak borunun patlamasına sebep olmuştur. (Kara, 2013, s. 40)

İlk Bilgisayar Solucanı (1988): 1988 yılında tüm dünyada İnternete bağlı bilgisayar sayısı yalnıza 60.000 civarında olmuştur. 2 Kasım 1988 tarihinde bu bilgisayarların çoğu aniden yavaşlamaya başlamıştır. (Siber Güvenlik Olayları) Morris solucanı dünyanın siber altyapısını etkileyen ilk solucan olmuştur. Büyük oranda ABD'deki bilgisayarlarda görülmüştür. Solucan, UNIX sisteminin Noun 1'deki zayıf noktaları kullanmış ve kendini düzenli olarak çoğaltmıştır. Solucan, bilgisayarları kullanılamaz hale gelene kadar yavaşlatmıştır. Solucan, İnternet'in ne kadar büyük olduğunu ölçmeye çalışan Cornell Üniversitesi öğrencisi Robert Tapan Morris tarafından oluşturulmuştur. Robert Tapan Morris aynı zamanda ABD'de bilgisayar dolandırıcılığı ve istismar eylemiyle mahkum edilen ilk kişi olmuştur. (NATO Review Magazine).

Körfez Savaşı'nda Siber Operasyon (1990): Körfez savaşı sırasında ABD Ordusu İstihbarat Birimi, telsiz frekansı tespit donanımları ile yüklü olan helikopterleri Irak sınırının güvenli kısmındaki bazı stratejik noktalara göndermiştir. Birim bu yöntemle Irak ordusunun iletişim sistemleri üzerinde çalışmış ve telsiz frekans sistemlerini tespit etmiştir. Operasyon başladığı andan itibaren Irak iletişim sistemi gizlici dinlenmiştir. Hatta sadece dinlemek ile de kalmayıp, bir müddet sonra iletişime geçmişlerdir. Irak ordusu kendi birimlerine telsiz ile talimat veremeyeceğini anladıktan sonra yedek frekans listesi üzerinden iletişime geçmeye çalışmıştır. Ancak Amerikan ordu helikopterlerinin içerisindeki donanımlar, yeni frekansları da tespit etmiştir. Bunun üzerine Irak ordusu birlikleriyle telsiz iletişimi yapmaktan vazgeçmiş ve gömülü telefon hatlarını kullanmaya çalışmıştır. Ordu istihbaratına tüm bilgiler eski temel seri telefon hatlarından herhangi birine şifreli vericiler ile girip gönderilmeye çalışılmıştır. Ancak Amerikan ordusu, telsiz iletişimini kesmekte kullandığı

yöntemi tekrar kullanmıştır. Son çare olarak, Iraklı subaylar talimatları yazarak göndermeye çalışmıştır. En ufak bir talimat bile arazideki Iraklı subaylara kamyonlarla gönderilip, cevapları kamyonlarla alınmaya çalışılmıştır. Birlikte hareket edilmesi ve talimatların birden fazla birime bu şekilde gidip gelmesi oldukça zorlaşmıştır. Ayrıca talimatları taşıyan kamyonların Amerikan ordusu tarafından hedef alınması, Iraklı şoförlerin mesaj taşımayı reddetmesine sebep olmuştur. İletişimin ele geçirilmesi ile beraber Irak komuta kontrol sistemi tamamen yıkılmıştır. Körfez Savaşı, savaşların geleneksel yöntemler yerine, siber ortam yetenekleri ile yürütülebileceğini, ordunun kalabalık olmasının çokta önemli olmadığını göstermiştir. Savaşta siber güvenliğin sağlanmasının önemli olduğunu, savaşta siber ortamın kaybedilmesi durumunda savaşın seyrinin değişebileceği ihtimalini gösteren, bir savaştaki ilk örnek olay olmuştur. (Kara, 2013, s. 41-42)

Truva Atları ile İlk Saldırı (1994): 1994 yılında kimliği belirlenemeyen siber saldırganlar Amerikan Hava Kuvvetleri'nin araştırma ve ana komuta üssü olan Rome üssüne yüzlerce izinsiz sızma gerçekleştirmişlerdir. Truva atlarını kullanarak üssün ağına sınırlandırılmamış bir şekilde erişmişler ve izlerini de yok etmeyi başarmışlardır. Siber saldırganlar pek çok gizli bilgiye erişmişlerdir. Bununla birlikte uzaktan erişim ile diğer kritik kurum veya firmalara Rome üssünden bağlanan güvenilir bir taraf gibi davranarak erişmeyi başarmışlardır. (Siber Güvenlik Olayları)

Bilgi Savaşının İlk Defa İnternet Ortamına Yansıması (1994): Rus askerleri Rusya'nın toprak bütünlüğünü sağlamak ve anayasayı uygulamak amacı ile Aralık 1994 tarihinde Çeçenistan'ın başkenti olan Grozni'ye girmişlerdir. Ağır silahlarla donatılmış olan Rus askerleri Çeçen direnişinin kısa süreceği düşünmüştür. Fakat Rusların beklentileri ile sahadaki gerçekler uyuşmamıştır. Soğuk Savaş'ın ardından silahlı çatışma, ilk defa internet ortamına yansımıştır. Başta internet olmak üzere bütün medya imkânlarını kullanan Çeçenler, bilgi savaşının (information war) ilk örneklerini ortaya koymuştur. Çeçenlerin internete yükledikleri ölü Rus askerlerin resimlerini gören anneler, çocuklarını kurtarmak için harekete geçmişlerdir. (Bıçakcı, 2012, s. 209) İnternetin savaş alanında kullanıldığı ilk örneğini teşkil eden bu olaydan sonra uluslararası sistemin aktörleri internet merkezli muhtemel saldırılara karşı hazırlık yapmaya başlamıştır. (Aydın (ed.), 2013, s. 30)

Red Hack Grubu'nun Ortaya Çıkışı (1997): Grup, 1997 yılında belirli bir tüzük ile kuulmuştur. 12 kişilik çekirdek kadrodan oluşmaktadır. Çekirdek kadro haricinde militanları da mevcuttur. Grup kendisini sosyalizme inanan bilişim alanındaki işçiler olarak nitelendirmektedir. Çekirdek kadro haricinde birbirlerini tanımamaktadırlar ve belli güvenlik önlemleri çerçevesinde iletişim kurmaktadırlar. Grup, interneti sadece bir araç olarak görüp, protestolarını sosyal medya üzerinden yapmaktadır. Türkiye'yi ve dünyayı ilgilendiren bir çok faaliyette bulunarak, siber dünyada neler yapılabileceğini göstermiştir. 2005 yılında sistemi hackleyerek İstanbul'daki bütün trafik cezalarını silmiştir. 2007 yılında MOBESE sistemine hackleyerek deşifre etmiştir. 2008 yılında Türkiye'deki bütün valilikler ait siteleri hackleyerek, Sivas Katliamı ile ilgili yazılar yazmıştır. 2012'de Emniyetin %95'ini hackleyip, çok sayıda iç yazışma ve ihbarı ortaya dökmüştür. (Kara, 2013, s. 21)

Ay Işığı Labirenti Operasyonu (1998): Dünya kamuoyunda moonlight moze operasyonu olarak bilinen operasyonda ABD'nin Enerji Bakanlığı, NASA Pentagon ve üniversitelere ait araştırma ve geliştirme sırları, askeri donanım tasarımları, askeri yapılandırmaları ve askeri tesislerin haritaları gibi birçok gizli bilgi çalınmıştır. Bilgilerin, Rus hackerlar tarafından çalındığı düşünülmesine karşın Rusya konu ile bağlantısının olmadığını belirtmiştir. (Kara, 2013, s. 42-43) Ne bulursam kardır düşüncesi ile internet üzerinden sızlamalar yapan hackerların değeri milyon dolarlar edebilecek devlet sırlarına bile ulaşabileceğini göstermiş önemli bir olaydır.

NATO'ya Yönelik İlk Siber Saldırılar (1999): NATO Genel Sekreteri Javier Solana'nın emirleri doğrultusunda Kosova'da bulunan Sırp hedeflerinin bombalanmaya başlaması ile birlikte üye ülkelerin askeri haberleşme sistemlerine ve NATO karargâhına yönelik siber saldırılar yapılmıştır. (Bıçakcı, 2012, s. 210) Sırpların ait Kara El (Black Hand) grubu İngiltere, ABD ve NATO askeri haberleşme sistemlerine yönelik siber saldırılar yapmıştır.

İsrail-Hizbullah Olayı (2000): İsrail askerlerinin Hizbullah tarafından kaçırılmasının ardından İsrail, Hamas ve Hizbullah sitelerine yoğun bir saldırı başlatmış, buna karşılık olarak Filistin taraftarı hackerlar da İsrail hükümetine ait sitelere saldırılar gerçekleştirmişlerdir. Karşılıklı münakaşa sonucu gruplar birçok siteyi çökertmişlerdir. Ardından Pakistan'daki Hackerz Club adında bir hacker grubu da olaya dahil olmuş ve ABD'de konuşlu İsrail taraftarı bir lobi olan AIPAC'ın sitesine girerek önemli olan iletişim ve kredi kartı bilgilerini ele geçirip ardından yayınlamıştır. Bu olay, yerel bir siber anlaşmazlığın çok kısa bir zamanda uluslararası hale gelebileceğini göstermesi açısından önemli bir örnek olmuştur. (Kaya, 2012, s. 52-53)

Avustralya Atık Sistemi Olayı (2000): Yazılım geliştirme şirketinde çalışan Avustralyalı bir hacker işinden ayrılmasından bir süre sonra Avustralya Queensland'da bulunan atık işleme tesislerinin kontrol sistemine sızmış ve 264.000 galon işlenmemiş atığı yakındaki park ve nehirlere yönlendirmiştir. (Kaya, 2012, s. 54) Bu olay ise çevre temizliğindeki güvenliğin bile siber güvenlikle ilişkili olduğunu göstermek açısından önemli bir örnek vaka olmuştur.

Hainan Adası Olayı (2001): ABD casus uçağının Güney Çin Denizi üzerinde bir Çin uçağı ile çarpışması sonucu Çin uçağı düşmüştür. Hasar alan ABD uçağı ise Hainan Adası'na inmek zorunda kalmıştır. Bunun üzerine ABD hükümetine karşı yaklaşık 80.000 Çinli siber saldırgan tarafından "ABD saldırganlığına karşı kendini savunma harekâtı" başlatılmıştır. Daha sonra bu olay The New York Times gazetesi tarafından Birinci İnternet Savaşı (World Wide Web War I) olarak nitelendirmiştir. (Çeliktaş, 2016, s. 53-54)

Code Red Solucanı'nın Ortaya Çıkışı (2001): Temmuz 2001 tarihinde ortaya çıkan bu solucan, ayın 1 – 19 arasında kendisini çoğaltacak, 20 – 27 arasında belirli bir siteye hizmet dışı bırakma saldırısı gerçekleştirecek ve 27'sinden ay sonuna kadar da bilgisayarda sessiz bir şekilde uyumaya programlanmıştır. Yaklaşık 300.000 bilgisayarı etkileyen bu solucan, ABD'de Microsoft'un IIS Web sunucularında bulunan bir güvenlik açığından faydalanmıştır. İlk türleri Beyaz Saray'ı belirli tarihlerde hizmet dışı bırakacak şekilde saldırı düzenlemeye programlanmıştır. Beyaz Saray'ın sistemi bu

saldırılardan korunmuştur ancak sitelerin hizmet verilemez hale gelmesinin önüne geçilememiştir. (Kaya, 2012, s. 54-55)

Titan Rain Olayı (2002): 2002 yılında Çinliler tarafından ABD Savunma Bakanlığı'na karşı başlatılan siber casusluk vakalarına verilen gayri resmi isimdir. Çinliler'in bu saldırılar sonucunda NIPRNet sunucularından 10 – 20 terabayt veriyi elde ettiği tahmin edilmektedir. Bu olay sonrası buna benzer olaylar Titan Rain ismi ile anılmaya devem etmiştir. (Kaya, 2012, s. 55)

En Büyük Askeri Bilgisayar Saldırısı (2002): Gary McKinnon, en büyük askeri bilgisayar saldırısı düzenleyen bir bilgisayar korsanıdır. NASA'nın ve ABD'nin silahlı kuvvetlerinin bilgisayarlarına erişmiştir. (Kara, 2013, s. 12) Amerikalılar bilgisayarlara 800.000$ değerinde zarar verdiğini iddia ediyorlar. İngiltere'de yaşayan McKinnon, ABD'ye teslim edilmemek için mücadele etmiştir. 2008'de McKinnon'a bir tür otistik asperger sendromu teşhisi konmuştur. (Gary McKinnon, 2012)

Siber Ortamın Psikolojik Harpte Kullanılması (2003): 2003 yılında ABD'nin Irak'ı işgali öncesinde Irak Savunma Bakanlığı e-posta sistemi hacklenmiş ve binlerce Irak subayına hiç savaşa girmeden teslim olmaları yönünde bir çağrı yapılmıştır. Çağrı amacına ulaşmıştır. ABD, Irak ordusunu konvansiyonel saldırı öncesinde bunu yapmıştır. Hackerların Irak savunmasının gizli ağına girerek göndermiş olduğu mesaj, subayları psikolojik olarak çökmesine sebep olmuştur. Eski usul kağıt broşür atma yönteminin artık başka bir yöne evrildiğini göstermiştir. (Kara, 2013, s. 45) Bu olay psikolojik propagandanın siber uzayda da yapılabildiğini göstermiştir.

Anonymous Grubu'nun Ortaya Çıkışı (2003): Bağımsız bir grup insanın 2003 yılında internet üzerinden birleşmesi ile oluşmuştur. Hactivist bir gruptur. Dünyanın her yerinden üyesi bulunmaktadır ve grubun üyeleri birbirini tanımamaktadır. Herkes Anonymous'a destek verebilir ve üyesi olabilir. Anonymous grubu, liderliğe ya da hiyerarşik bir düzene karşıdır. Anonymous, internet özgürlüğünü savunmaktadır. Grup, adını ilk kez Sony operasyonu ile duyurmuştur. Amerikan ordusuna hizmet veren Lockheed Martin şirketinin enformasyon ağına saldırı düzenlemiştir. Grup, 8 Aralık 2010'da MasterCard ve Visa'ın sitelerini çökertmiştir. 2011'de İrlanda'daki yerel seçimlerinde bir partinin web sitesini ele geçirerek, siteye mesaj bırakmıştır. Arap Baharı'na destek veren anonymous grubu, Tunus'ta yaşanan devrim sırasında Tunus'lu hackerlar ile birlikte devlet ait sekiz web sitesini çökertmiştir. (Kara, 2013, s. 19)

NASA'ya Saldırı (2006): NASA uzay mekiğini fırlatmadan önce sisteme girildiği korkusu ile eklentili e-postaları engellemiştir. En son uzay aracının planlarının ise bilinmeyen yabancılar tarafından elde edildiğini bildirmiştir. (NATO Review Magazine)

Shady RAT Saldırıları (2006-2011): İlk kez 2011 yılında McAfee adlı antivirüs şirketi tarafından hazırlanan bir rapor ile varlığı öğrenilmiştir. 2006 ile 2011 yılları arasında yapılmış olan Shady RAT (Uzaktan Yönetim Aracı-Remote Administration Tool) saldırıları, APT türündeki casusluk eylemleri olmuştur. Bu saldırılar ile 70'in üzerinde kurum, kuruluş ve şirket hedef alınmıştır. Uluslararası piyasalarda rekabet açısından şirket sırları, stratejileri, planları ve ekonomik başarılarının vs. meselelerin son derece önemli olduğu göz önüne alınırsa, böyle bir eylemin sonuçlarının dünya piyasası üzerinde

oldukça etkili olacağı aşikârdır. Shady RAT saldırıları süresi ve etki çapı bakımından, şu ana kadar yapılmış en geniş çaplı siber saldırı türüdür. (Çeliktaş, 2016, s. 58)

En Kapsamlı Siber Bilgi-Banka Soygunu (2007): Amerika'da ev eşyaları şirketi olan TJX firması, bir sızma saldırısının kurbanı olduğunu açıklamıştır. Siber saldırganlar tarafından şirketin ürün iade bilgisi, banka kartı ve kredi kartı bilgilerinin saklandığı sisteme erişilmiştir. 46 milyon civarında müşteriye ait kritik bilgi, siber saldırganlar tarafından ele geçirilmiştir. (Siber Güvenlik Olayları)

İsrail'in Orchard Operasyonu (2007): İsrail, Orchard operasyonunda F-15 ve F-16 uçakları ile Suriye'nin son teknoloji hava savunma sistemlerine yakalanmadan, Suriye içerisinde bulunana Suriye ve Kuzey Kore'nin ortak nükleer tesisini bombalamıştır. İsrail'in Suriye'deki Rus yapımı hava savunma sistemlerini ele geçirmesi sonucu böyle bir durum ortaya çıktığı düşünülmektedir. Bu olay son teknoloji ile üretilmiş olan ve çok yüksek güvenlilik sağladığı düşünülen savunma sistemlerinin bile siber saldırılar sonucunda nasıl çalışamaz duruma getirilebildiğinin bir kanıtı olmuştur. (Çeliktaş, 2016, s. 55)

Estonya Hükümet Ağına Saldırı (2007): Estonya'da bulunan bronz bir asker heykelinden oluşan bir savaş anıtını kaldırılması konusunda Estonya'nın Rusya ile olan münakaşası üzerine Estonya yabancı saldırganlar tarafından ulusal bilgi sistemleri, internet hizmet sağlayıcıları ve bankalara yönelik geniş katılımlı ve koordineli DDoS (Distrubuted Denial of Service) saldırıları, devlete ait bazı web sayfalarının ele geçirilmesi ve spam (yığın e-posta) saldırıları ile karşı karşıya kalmıştır. Estonya'nın hükümet ağı servis durdurma saldırısı ile engellenerek bazı servisler günlerce çalışmamıştır. Estonya bu olay sonrası Avrupa Birliği içerisinde siber güvenlik stratejisini belirleyerek savunmasını geliştirmeye çalışan ilk ülke olmuştur. Estonya olayı, siber uzayın, politik amaçlar uğruna kullanılmaya başlandığının ve bu ortamı artık devletlerin rekabet alanı olarak gördüklerinin bir miladı olmuştur. (Çakmak & Demir, 2009, s. 122) Bu saldırı uluslararası ilişkilerde de siber güvenlik anlamında bir kırılma noktası olmuştur. Çünkü siber savaş senaryolarının sadece birer komplo teorisi olmadığı anlaşılmıştır. Bunun üzerine NATO başta olmak üzere AGİT ve BM gibi birçok kurum siber uzayı da dikkate alarak güvenlik politikalarını revize etmeye başlamıştır. (STM, 2016, s. 4)

ABD Savunma Bakanlığı'nın e-posta Hesaplarına Saldırısı (2007): Kimliği tespit edilemeyen yabancı bilgisayar korsanları tarafından Pentagon'un ağına sızmak amacı ile ABD Savunma Bakanlığı'nın gizli olmayan e-posta hesabı yapılan bir dizi saldırı sonunda kırılmıştır. (Siber Güvenlik Olayları)

Çin'de Casus Yazılımlar (2007): Çin Devlet Güvenlik Bakanlığı, %25'inin Tayvan'dan, %42'sinin ABD'den olduğunu iddia ettiği yabancı hackerların Çin'in önemli alanlarından bilgi çaldıklarını söylemiştir. 2006'da Çin Havacılık ve Uzay Bilimi ve Endüstri Kurumu (CASIC) internet ağı incelendiği zaman, gizli bölümlerin ve kurumsal liderlerin bilgisayarlarında casus yazılımlar bulunmuştur. (NATO Review Magazine)

Gürcistan Bilgisayar Ağı'na Saldırı (2008): Rusya ile Gürcistan arasında olan anlaşmazlık sırasında yabancı korsanlar tarafından Gürcistan'ın bilgisayar ağına sızılmış ve hükümet web sunumcularına Graffiti resmi

koyulmuştur. Rusya, geleneksel savaş yöntemleri ile eş zamanlı olarak siber saldırıları da başlatmıştır. Rusya tarafında olan hackerlar Gürcistan'da trafiği destekleyen tüm yönlendiricileri ele geçirmiştir. Somut bir zararı olmayan bu olay Gürcistan hükümeti üzerinde politik baskı oluşturmuştur. Siber saldırıların gerçekleştirildiği siteler incelendiğinde bunların ABD'den çalınan kredi kartları ile Türkiye ve Rusya'da açılan siteler olduğu belirlenmiştir. Gürcistan'a yönelik siber saldırıların siber güvenlik açısından ortaya koyduğu en önemli sonuç bunun gerçek bir hibrit savaş niteliğinde olması olmuştur. (Bıçakcı, 2012, s. 219)

Kuantum Kriptografi (2008): 12 Avrupa ülkesinin işbirliği ile dünyanın ilk quantum kriptografi kullanan ticari iletişim ağı 2008 yılında kullanıma açılmıştır. (Siber Güvenlik Olayları)

İsrail İnternet Alt Yapısına Saldırı (2009): İsrail, Gazze şeridine Ocak 2009 tarihinde askeri saldırı yapmıştır. Bunun paralelinde de İsrail'in internet alt yapısına siber saldırı yapılmıştır. Yaklaşık olarak 5 milyon bilgisayarda çalışan hükümet web sitelerine karşı yapılmıştır. Hizbullah veya Hamas tarafından finanse edilen Sovyet suç örgütlerinin yaptığına inanılmıştır. (NATO Review Magazine)

Aaron H. Swartz'ın Bilgi Korsanlığı (2009): Amerikan federal mahkemelerine ait PACER veritabanında bulunan yaklaşık olarak 18 milyon belge Aaron H. Swartz tarafından 2009 yılında indirilip, para karşılığı satılıp, internette yayınlamıştır. Ardından 2011 yılında, MIT Üniversitesinin bilgisayarlarını kullanarak, çevrimiçi olarak akademik dergileri arşivlemede kullanılan bir sistem olan JSTOR (Journal Storage)'dan 4 milyona civarı belge, makale ve kitabı bilgisayarına indirilip, internet üzerinden paylaşılmıştır. Aaron H. Swartz , yasadışı dosya indirme ve bilgi korsanlığı suçlarından yargılanmış ve 35 yıl hapis cezasına çarptırılması beklenirken 2013 yılında kendini asmıştır. (Kara, 2013, s. 18)

Çin'deki Arama Makinesi Badiu'ya Saldırı (2010): İran Siber Ordusu olarak adlandırılan bir grup, Çin'in arama makinesi olan Badiu'nun servisini bozmuştur. Kullanıcılar İran'ın politik mesajını içeren başka bir servise yönlendirilmiştir. Aynı grup daha sonra benzer bir mesajla Twitter'a da saldırmıştır.

Wikileaks Belgeleri (2010): Wikileaks kendisini kar amacı gütmeyen bir medya kuruluşu olarak tanımlamakta, asıl amacının önemli bilgi ve haberleri kamuoyuna iletmek olduğunu belirtmektedir. Wikileaks'in ABD başta olmak üzere, devletlerin gizli politikalarını dünya kamuoyu ile paylaştığı görülmüştür. (Karakuzu, 2015, s. 78) ABD'nin kıdemli bir eri olan Bradley Manning, ordu veri tabanından indirdiği görüntüleri ve dokümanları, 1966-2010 yılları arasında ABD Dış İşleri Bakanlığı'nın yapmış olduğu gizli yazışmaları, Kasım 2010 tarihinde Wikileaks sitesine sızdırmıştır. ABD Büyükelçilikleri tarafından gönderilen yaklaşık 250.000 gizli diplomatik belge internet sitesi üzerinden yayımlanmıştır. (Karakuzu, 2015, s. 77) Ardından Julian Assange ve kurucusu olduğu Wikileaks sitesi hakkında sansüre karar verilmiştir. İnternetin özgürlüğünü savunan hacker grubu Anonymous ise sansüre karşı tepki ortaya koymuştur. Yayınlanan görüntüler içerisinde en çok dikkat çeken ise Cenevre Sözleşmesi'ne göre sivil hedeflerin bombalanamayacağı kuralını ihlal eden görüntülerin yer alması olmuştur. (Kara, 2013, s. 17)

Stuxnet Virüsü'nün Fark edilmesi (2010): İran'ın nükleer santrifüjlerinin beşte biri Stuxnet adıyla bilinen bilgisayar kurdu tarafından saldırıya uğramıştır. Uranyum zenginleştirmede kullanılan santrifüjler son derece hızlı dönen makinelerdir. Virüsün amacı, santrefüjlerin kontrolünde kullanılan Programlanabilir Mantık Denetleyicisi (PLC-Programmable Logic Controller) kontrol devrelerini hedef alarak kontrolü ele geçirmekti. Kontrolör yazılımı bozulmaya başlayınca hızla dönen makinelerin dönme hızı kontrolden çıkıp, makineler parçalanmaya başlamıştır. Stuxnet, endüstriyel PLC'leri bozacak komutlar üretiyor ve PLC'lerin sanki normal operasyon yapıyormuş gibi geri bildirim vermelerini sağlayarak bozulma sürecini saklayabilmiştir. Bu nedenle verilen zarar uzun zaman sonra anlaşılabilmiştir. İran'a yapılan bu saldırının arkasında İsrail ve Amerika olduğu kanaati olmasına karşın kamuya karşı taraflarca bir açıklama yapılmamıştır. Haziran 2010'da varlığı fark edilen virüs İran'daki Natanz ve Buşehr şehirlerinde bulunan nükleer tesisleri etkilemiştir. (Bıçakcı, 2012, s. 218) Barajlar, sanayi birimleri ve enerji santralleri gibi altyapı tesislerinin sistemlerini hedef alan ilk kötü amaçlı yazılım olan Stuxnet virüsü ülke genelinde yaklaşık 30 bin sanayi bilgisayarını etkilemiştir. (Özçoban, 2014, s. 57) Siemens endüstriyel kontrol sistemlerine müdahale etmek için tasarlanmış karmaşık bir kötü amaçlı yazılım parçası olan Stuxnet İran, Endonezya ve başka yerlerde keşfedimiş ve İran'ın nükleer programına yönelik bir hükümet siber silahı olduğu yönünde spekülasyonlara yol açmıştır. (NATO Review Magazine) New York Times haberine göre Stuxnet, İran'da 5000 adet santrifün 1000 tanesini devreden çıkarmıştır ve İran nükleer programını 1,5 ila 2 yıl ertelemiştir. Bu saldırı, Bush hükümeti tarafından başlatılan ve "Olimpiyat Oyunları" kod adı verilen siber saldırıların Obama hükümeti sırasında hızlanan devamı niteliğinde olmuştur. (Obama Order Sped Up Wave of Cyberattacks Against Iran, 2012)

Duqu Virüsü'nün Ortaya Çıkışı (2011): Duqu virüsü, Stuxnet virüsüne benzemektedir. Bu virüsün Stuxnet virüsünün yazarları tarafından yazılmış olabileceği veya Stuxnet virüsünün kaynak kodunu bir şekilde inceleme imkanı bulanlar tarafından yazılabileceği düşünülmektedir. İki virüsün ortak özelliği hedeflerinde endüstriyel kontrol sistemleri olmasıdır. Duqu virüsü Stuxnet virüsünden farklı olarak SCADA sistemleri ile ilgili kritik bilgileri toplamak için tasarlanmıştır. Otuzaltı gün sonra virüs eriştiği sistemden kendisini silmektedir. Duqu virüsü saldırı yapacağınız sistemin zayıf ve güçlü yönlerini ele geçirmek için SCADA sistemleri ile ilgili kritik bilgilerin tespiti yapmaktadır. Bu tespit ise Stuxnet benzeri saldırı silahlarının işini ve oluşumunu kolaylaştırmaktadır. Bu sebeple, Duqu virüsü, gelecek için büyük tehlikeler ve kaygılara sebep olmaktadır. (Kara, 2013, s. 35)

ABD Savunma Bakanlığı'nın Savunma Müteahhidine Saldırı (2011): ABD Savunma bakanlığı savunma müteahhidine karşı yapılan saldırı sonunda, savunma bölümünden 24.000 adet dosya çalındığı bildirilmiştir. (Siber Güvenlik Olayları)

Kanada'da Bakanlıklara Saldırı (2011): Kanada hükümeti, Kanada Ulusal Savunma Bakanlığı araştırma ajansı da dahil olmak üzere ajanslarına karşı büyük bir siber saldırı düzenlediğini bildirmiştir. Saldırı, Kanada'nın ana ekonomi kuruluşları olan Maliye ve Hazine Bakanlıklarının internet'ten ayrılmasına yol açmıştır. (NATO Review Magazine)

Flame Virüsü'nün Fark Edilmesi (2012): Flame virüsünün ne zaman ortaya çıktığı bilinmemektedir fakat fark edilmesi 2012 yılında olmuştur. Stuxnet virüsünden 20 kat daha karmaşık bir kodla yazılmıştır. Flame Virüsü'nün bilginin sızdırılabilmesi için monitör, klavye, depolama cihazları, mikrofon, USB, Bluetooth ve Wi-Fi gibi her türlü sistem işlemcilerini ve donanımını kullabildiği Budapeşte'de bulunan bir Kriptografi ve Sistem Güvenliği Laboratuvarı (CrySyS Lab) tarafından yapılan araştırma sonucu ortaya koyulmuştur. Flame Virüsü'nü yönlendirmek için virüsün arkasında bulunan kişiler tarafından kontrol ve komutası çok sık değişen bir ağ kullanılmıştır. İran, İsrail, Mısır, Suriye, Batı Şeria, Lübnan, Sudan ve Suudi Arabistan virüsten etkilenen bölgeler arasında gösterilmektedir. (Kara, 2013, s. 36) Flame virüsü, siber casusluk amacı ile geliştirilen en güçlü siber silahlardan biridir. (Aydın, 2012, s. 25)

Gauss Virüsü'nün Fark Edilmesi (2012): Gauss diğer yazılımlardan farkı bankaları etkilemesidir. Siber bir tehdit olan virüs çevrimiçi bankacılık hesaplarını izlemiştir. Virüs, etkisine aldığı bilgisayarlarda bulanan çevrimiçi bankacılık hesap kimlik bilgileri, hassas verileri ve tarayıcı parolalarını çalmak için tasarlanmıştır. (Kara, 2013, s. 36)

Shamoon Virüsü (2012): Virüsün ortaya koyulmasındaki amaç enerji sektörünü hedef almak olmuştur. Virüs işleme mantığı bulaştığı sistemlere zarar vermek ve bilgisayarları kullanılamaz hale getirmek olmuştur. 2012 yılında Suudi Arabistan'ın Aramco adlı ulusal petrol şirketine yapılan bir siber saldırı ile varlığı anlaşılmıştır.Yapılan saldırı ile petrol şirketine ekonomik zarar verilmiştir. Araştırmacılar ve anti-virüs şirketleri virüsün hedefinde petrol endüstrisinin olabileceğini düşünmüşlerdir. (Kara, 2013, s. 37-38)

Kırmızı Ekim Siber Saldırısı (2012): Rus firması olan Kasperski, Kırmızı Ekim denilen ve 2007'den beri dünya çapında çalışan bir siber saldırıyı tespit etmiştir. Micrsoft Word ve Excell programlarında bulunan bir açıklıktan yararlanan bilgisayar korsanları, askeri tesisler, hükümet elçilikleri, enerji sağlayıcılar, nükleer tesisler, araştırma firmaları ve diğer kritik alt yapılar hakkında bilgi toplamışlardır.

Güney Kore Finans Kurumlarına Saldırı (2013): Koreli yayıncı YTN'nin yanı sıra, Güney Kore finans kuruluşları, Kuzey Kore'nin geçmişteki siber çabalarına benzer bir olayla ilgili ağlarının etkilediğini söylemiştir.

Küresel Dinleme Skandalı (2013): Amerikan Ulusal Güvenlik Kurumu'nda bulunan Edward Snowden, binlerce gizli belgeyi kamuya açıklamıştır. Bu belgeler Ulusal Güvenlik Kurumu'nun, Google'ın veri merkezleri arasındaki hatları dinlemekte ve kişisel bilgilere erişmekte olduğunu ortaya çıkarmıştır. Ayrıca ABD Ulusal Güvenlik Kurumu , NIST'ın bir şifreleme standardında bilinçli olarak açık kapı bırakılmasını sağlamış ve bu standardı kullanan şifreleme sistemlerinin şifrelediği bilgileri kolayca çözebilmiştir. (Siber Güvenlik Olayları)

Black Energy ve Kill Disk Truva Atı'nın Etkisi (2015): Black Energy truva atı, ilk kez 2007 yılında basit DDoS saldırılarında tespit edilmiştir. Ardından banka dolandırıcılığı ve spam göndermek gibi amaçlarla kullanılmaya başlanmıştır. 2014 yılında ise yerleştirildiği bilgisayarlarda ağ keşfi yapma, sabit sürücülerinden veri toplama ve bilgisayarın uzaktan yönetilmesini sağlayan arka kapı niteliğinde olan zararlı bir yazılımdır. Kill Disk truva atı ise

sabote etmek, kritik sistemleri kapatabilmek ve sistemin yeniden başlatılmasına engel olmak için sistem dosyalarını silebilmek gibi yeteneklere sahip zararlı bir yazılımdır. En çok Ukrayna'da görülmekle birlikte Polonya'daki birçok özel kurum, devlet kuruluşu ve sivil organizasyonların bilgisayarlarında da görülmüştür. Black Energy ve Kill Disk truva atı birlikte kullanılarak 23 Aralık 2015 tarihinde Ukrayna'da enerji dağıtım şirketlerine yapılan siber saldırılar yapılmış ve yaklaşık olarak 800 bin kişi elektriksiz bırakılmıştır. (Çeliktaş, 2016, s. 58)

Türkiye'ye Yönelik Siber Saldırılar (2015): Türkiye, Aralık 2015 tarihinde 6 ayrı "DNS Sunucusu" saldırıya uğramış ve tarihinin en büyük siber saldırıları ile karşı karşıya kalmıştır. DDoS saldırıları aracılığı ile DNS sunucularının internet hizmetinin engellenmesi amaçlanmıştır. Gerçekleşen bu saldırılar neticesinde "com.tr", "gov.tr" ve "edu.tr" benzeri "tr" uzantılı yaklaşık 400 bin siteye 1 hafta boyunca girişlerde sorun yaşanmış yada hiç girilememiştir. Anonymous adlı hacker grubu saldırıları üstlenmiştir. Fakat Uzmanlar bu çapta saldırıların arkasında bir devlet desteğinin bulunması ihtimalinin yüksek olduğunu savunmuşlardır. (Çeliktaş, 2016, s. 59) Fail tam olarak belirlenemese de 24 Aralık 2015 tarihi, 24 Kasım'da Rus uçağının düşürüldüğü tarihten tam bir ay sonrasına denk geldiği için tahmin okları Rusya'yı göstermiştir. (Haber Hergün, 2015)

Siber Uzay'da Terör Propagandası (2016): ABD yönetimi, IŞİD'in siber faaliyetler ve propaganda amaçlı kullandığı unsurlara yönelik 2016 yılında kapsamlı bir operasyon icra etme kararı almıştır. (Kasapoğlu, 2017, s. 1) Operation Glowing Symphony adı verilen siber operasyondaki kritik bir detay ABD yönetiminde görüş ayrılıklarına neden olmuştur. Siber saldırı düzenlenecek IŞİD hedeflerinin bulunduğu ülkelerin içerisinde ABD'nin partnerleri ve müttefikleri bulunması üzerine ABD yönetiminde istihbarat-işbirliği kanalları üzerinden haber verilip verilmemesi gerektiği üzerine görüş ayrılığı meydana gelmiştir. (U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies, 2016)

III. Sonuç

Siber uzay sunduğu imkanlar kadar içerisinde güvenlik açıklarını da barındırır. Siber uzaya güvenlik açıklarının farkında olarak yaklaşmak gerekir. Kritik altyapılara siber ortamdan gelebilecek tehditlerin, milyonlarca insanın faydalandığı sistemleri ve dolayısıyla insan hayatını risk altına sokmaya başlamasıyla beraber siber güvenlik göz ardı edilemez bir kaygı olmuştur. Özel mülkiyetlerde nasıl güvenlik tedbirleri alınıyor, kapılar kilitleniyor, alarm ve değişik emniyet tedbirlerine başvuruluyor ise siber alanda da güvenlik kaygısı öncelikli olarak göz önüne alınmalıdır. Siber güvenlik vakaları ciddiyetleri yükselerek artmaya devam etmektedir. Bu ciddiyetin farkında olup daha büyük felaketlere sebep olunmasının önüne geçilmelidir.

İnsan, eğitim ve teknoloji birlikteliği siber güvenlikte temel bileşenlerdir. Siber güvenlikte gizlilik, bütünlük ve erişilebilirlik ise temel omurgadır. Konu ile ilgili yüksek farkındalığın oluşturulması, konunun uzmanı yöneticilerin bulunması, ağ bilgi sisteminin güvenliğinin ciddiye alınması, neyin ve nasıl korunacağının/korunamayacağının bilinmesi, izleme ve denetim sistemlerinin oluşturulması, güvenliği artıracak unsurlardır. Fakat siber güvenlik

sağlanırken güvenlik-özgürlük dengesi iyi korunmalı, insan haklarına riayet edilmelidir.

Siber uzay dünya dengelerini değiştirebilecek bir meseledir. Siber uzayda, deyimi yerindeyse aslanı kediye boğdurmak mümkündür. Herkes siber uzayın bir aktörü olabileceği gibi çok düşük maliyelerle çok büyük zararlar verebilir. Siber güvenlik üzerinde küresel olarak işbirliği sağlanması gereken, ortak siber güvenlik politikasına ve hukukuna ihtiyaç duyan bir meseledir. Fakat bu konuda bir girişim olmaması sebebi ile herkes kendi başının çaresine bakmak durumunda kalmıştır.

Kaynakça

Akyeşilmen, N. (2016, Kasım 7). Siber Güvenlik ve Özgürlük. 11 7, 2017 tarihinde İlk Ses Gazetesi: http://www.ilksesgazetesi.com/yazar/siber-guvenlik-ve-ozgurluk-3816.html adresinden alındı

Aydın (ed.), M. (2013). 21.Yüzyılda Siber Güvenlik. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Aydın, F. (2012, Eylül). Türkiye'nin Ulusal Korunmasında Siber Güvenlik. Yayınlanmış Yüksek Lisans Tezi, Matematik ve Bilgisayar Bölümü .

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. Uluslararası İlişkiler , 9 (34), 205-226.

Boyraz, M. (tarih yok). NATO'nun Siber Güvenlik Politikası: Tarihsel Süreç ve Kırılma Noktaları. 11 5, 2017 tarihinde http://researchturkey.org/tr/natos-cyber-security-policy-the-historical-process-and-critical-junctures/ adresinden alındı

Çakmak, H., & Demir, C. K. (2009). Siber Dünyadaki Tehdit ve Kavramlar. H. Ç. (Ed.) içinde, Suç, Terör ve Savaş Üçgeninde Siber Dünya (1.Baskı b., s. 23-54). Ankara: Barış Platin Kitabevi.

Çeliktaş, B. (2016, Mayıs). Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme. Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü . Trabzon.

Choucri, N. (2012). Cyberpolitics in International Relations. London, England: The MIT Press.

Gary McKinnon. (2012, Aralık 14). 12 2, 2017 tarihinde BBC: http://www.bbc.com/news/uk-19946902 adresinden alındı

Güngör, U., & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. Karadeniz Araştırmaları , 14 (55), 131-146.

Gürkaynak, M., & İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi , 16 (2), 263-279.

Haber Hergün. (2015, 12 28). 11 30, 2017 tarihinde Siber saldırı değil savaş!: http://www.haberhergun.com/bilim-teknoloji/siber-saldiri-degil-savas-h41902.html adresinden alındı

habertobb. (tarih yok). Ekonomik Forum. 11 6, 2017 tarihinde habertobb: http://haber.tobb.org.tr/ekonomikforum/2015/251/012_021_KAPAK_KONUSU.pdf adresinden alındı

Kara, M. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü . İstanbul.

Karabulut, B. (2009). Küreselleşme Sürecinde Güvenlik Alanında Değişimler: Karadeniz'in Güvenliğini Yeniden Düşünmek. Karadeniz Araştırmaları , 6 (23).

Karakuzu, Ö. (2015, Nisan). Bilgi Toplumu Dönüşüm Sürecinde E-Devlet Kavramının Siber Ülke Güvenliği Açısından Değerlendirilmesi. Yayınlanmış Yüksek Lisans Tezi . Malatya: İnönü Üniversitesi, Sosyal Bilimler Enstitüsü.

Kasapoğlu, C. (2017, Haziran). Siber Güvenlik:Beşinci Boyutu Anlamak. Edam; Centre for Economics and Foreign Policy Studies (1) .

Kaya, A. (2012). Siber Güvenliğin Milli Güvenlik Açısından Önemi. Yayınlanmış Yükseks Lisans Tezi . Ankara: Kara Harp Okulu, Savunma Bilimleri Enstitüsü, Güvenlik Bilimleri Anabilim Dalı.

Knake, R. K. (2010). Internet Governance in an Age of Cyber Insecurity. 11 27, 2017 tarihinde Council Special Report, No:56: http://i.cfr.org/content/publications/attachments/ Cybersecurity_CSR56.pdf adresinden alındı

Kurnaz, İ. (2016). Siber Güvenlik ile İlintili Kavramsal Çerçeve. Cyberpolitik Journal , 1 (1), 56-77.

NATO Review Magazine. (tarih yok). 11 26, 2017 tarihinde NATO: https://www.nato.int/docu/review/2013/Cyber/timeline/TR/index.htm adresinden alındı

Obama Order Sped Up Wave of Cyberattacks Against Iran. (2012, Haziran 1). 11 30, 2017 tarihinde The New York Times: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all adresinden alındı

Öğün, M. N., & Kaya, A. Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. Güvenlik Stratejileri , 9 (18), 145-181.

Özçoban, C. (2014). 21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü. Harp Akademileri Stratejik Araştırmalar Enstitüsü . İstanbul.

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl? Uluslararası Bilgi Güvenliği Mühendisliği Dergisi , 2 (2), 10-17.

Siber Güvenlik. (tarih yok). 6 11, 2017 tarihinde İstanbul İl Sağlık Müdürlüğü: http://www.istanbulsaglik.gov.tr/w/anasayfalinkler/belge/siber_guvenlik_sunum.pdf adresinden alındı

Siber Güvenlik Olayları. (tarih yok). 11 26, 2017 tarihinde Kamu Siber Güvelik Derneği: http://kamusgd.org.tr/faydali-bilgiler/ adresinden alındı

Singer, P. W., & Friedman, A. (2014). Cyber Security and Cyber War : What Everyone Needs to Know. New York: Oxford University Press.

STM. (2016). Türkiye Siber Tehdit Durum Raporu. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.

U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies. (2016, Mayıs 9). 11 30, 2017 tarihinde The Washington Post: https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.eaa5b2dcfce7 adresinden alındı

Uçar, O. (2011). Siber Tehditler ve Savunma Yöntemleri. Bilgi Güvenliği Akademisi .

Ünver, M., & Canbay, C. (2010). Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik. Elektrik Mühendisliği (438).

(tarih yok). 5 11, 2017 tarihinde Türk Dil Kurumu: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.59ff1bb3b3c045.97324629 adresinden alındı