ANKARA
HACI BAYRAM VELİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MİLLİ GÜVENLİK AÇISINDAN SİBER GÜVENLİK

Semih POLAT

Tez Danışmanı
Prof. Dr. Hamit Emrah BERİŞ

YÜKSEK LİSANS TEZİ
AMME İDARESİ ANABİLİM DALI
GÜVENLİK YÖNETİMİ

ŞUBAT - 2020


HBM

MİLLİ GÜVENLİK AÇISINDAN SİBER GÜVENLİK

Semih POLAT

YÜKSEK LİSANS TEZİ
AMME İDARESİ ANABİLİM DALI
GÜVENLİK YÖNETİMİ BİLİM DALI

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ŞUBAT - 2020

Semih POLAT tarafından hazırlanan "Milli Güvenlik Açısından Siber Güvenlik" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / ~~OY ÇOKLUĞU~~ ile Ankara Hacı Bayram Veli Üniversitesi Amme İdaresi Anabilim Dalında Güvenlik Yönetimi Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Hamit Emrah BERİŞ
Siyaset Bilimi ve Kamu Yönetimi, Hacı Bayram Veli Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/~~onaylamıyorum~~ .....

Başkan : Doç. Dr. Tuncay ÖNDER
Siyaset Bilimi ve Kamu Yönetimi, Hacı Bayram Veli Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/~~onaylamıyorum~~ .....

Üye : Doç. Dr. Y. Furkan ŞEN
Güvenlik Yönetimi, Polis Akademisi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/~~onaylamıyorum~~ .....

Tez Savunma Tarihi: 04 /02/2020

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Figen ZAİF
Enstitü Müdürü

ETİK BEYAN

Ankara Hacı Bayram Veli Üniversitesi Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Somih POLAT

04.02.2020

Milli Güvenlik Açısından Siber Güvenlik

Yüksek Lisans Tezi

Semih POLAT

ANKARA HACI BAYRAM VELİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Şubat 2020

ÖZET

Hayatın her alanında karşımıza çıkan, gündelik yaşantımıza getirdiği bilgiye ulaşım, bankacılık, iletişim vb. alanları veya sosyal medya düzeyinde de olsa herkesin içerisinde olduğu siber uzayın barındığı tehlikeler göz ardı edilmemelidir. Siber uzayda saldırganın bilgisayar başında paranızı çalması, bir hırsızın sizden paranızı alma ihtimalinden günümüz şartlarında daha fazla, daha kolay ve daha az risklidir. Bu siber uzayın bireysel olarak getirdiği güvenlik sorunudur. Devletler ve kurumlar içinse bu tehlike maddi unsurlarında ötesinde, devlet güvenliği veya toplumsal sorunlara dönüşebilmektedir. Sürekli değişen siber uzayın yetenekleri olumsuz yönde de değişmekte yeni siber silahlar, yeni siber saldırı türleri ile farklı tarzlarda karşımıza çıkmaktadır. Bu değişim göz önünde bulundurularak güvenlik tedbirleri alınmalı, yaşanmış siber saldırılardan dersler çıkarılmalı, vatandaşların ve personelin sistemden zarar görmemesi ve sistemde açık oluşturmaması için bilinçlendirme faaliyeti yürütülmelidir. Ve en önemlisi bu siber güvenlik yaklaşımları sürekli hale gelmesi için milli güvenlik politikasına dönüştürmelidir.

Bilim Kodu : 111618
Anahtar Kelimeler : Siber, Milli Güvenlik, Siber Güvenlik, Siber Suç
Sayfa Adedi : 91
Tez Danışmanı : Prof. Dr. Hamit Emrah BERİŞ

Cyber Security in Terms of National Security

M.Sc. Thesis

Semih POLAT

ANKARA HACI BAYRAM VELİ UNIVERSITY

GRADUATE SCHOOL FOR ANKARA HACI BAYRAM VELİ UNIVERSITY

February 2020

ABSTRACT

The dangers of the cyber space that everyone is in, even in areas such as access to information, banking, communication, etc. or social media, should not be ignored. In cyber space, the attacker's stealing your money with cyber attack is more easy, and risk-free, in today's conditions than the possibility of a thief stealing your money from you. This is the individual security problem of cyber space. For states and corporation, this danger can turn into national security or social problems beyond financial damage. The capabilities of the ever-changing cyber space are changing in a negative way with new cyber weapons and new types of cyber attacks. Considering this change, security measures should be taken, lessons should be learned from the cyber attacks, awareness raising activities should be carried out in order to prevent the damage of citizens and awareness-raising activities should be carried out to prevent people from causing system deficits. And most importantly, these cyber security approaches should be transformed into national security policy for becoming permanent.

Science Code : 111618
Key Words : Cyber, National Security, Cyber Security, Cyber Crime
Page Number : 91
Supervisor : Prof. Dr. Hamit Emrah BERİŞ

İÇİNDEKİLER

Sayfa

Sayfa

TABLOLARIN LİSTESİ

Tablo **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

GRAFİKLERİN LİSTESİ

Grafik **Sayfa**

1. GİRİŞ

Güvenlik ihtiyacı sadece günümüzün değil tarih boyunca bütün insanların ve medeniyetlerin en temel ihtiyacı olagelmiştir. İnsanlık tarihi süresince fiziksel ihtiyaçlar sonrasında artan nüfus, gelişen toplum yapıları (köy, şehir, derebeylik, devlet vs.) güvenliği, güvenlik ihtiyacının ön plana getirmiştir. Maslow'un ihtiyaç piramidinde de güvenlik ihtiyacı fizyolojik ihtiyaçlar sonrasında ikinci en temel ihtiyaç olarak yer almıştır. Tarihin seyri süresince farklı boyutları ile karşımıza çıkan ve ihtiyacın ötesinde boyut kazanarak devlet politikası haline gelen güvenlik kavramının gelişme ve ilerleyişi teknoloji ile 4 fiziksel boyutun dışında 5. farklı bir boyuta daha taşınmıştır. Fiziksel boyutlardan farklı olarak insan eliyle oluşturulan siber uzay her an genişlemeye ve insanların hayatının her boyutunda yer almaya başlamıştır.

Ulaşım, haberleşme, internet ağlarının küresel ölçeklere ulaşması 'küresel köy' kavramını dünyanın önemli bir bölümü için gerçekleştirmiştir. Bu büyüme siber uzayı toplumsal yapımızın önemli unsurlarından biri haline getirmiştir. Türkiye nüfusunun bir önceki döneme göre % 9 oranında 5 milyon kişilik artış göstererek %72 oranında internet kullanıcısı olduğu, % 63 oranında aktif sosyal medya hesabı sahibi olduğu ve bu kullanıcıların günlük ortalama internet kullanımın 3 saatin üzerinde olduğu günümüzde yeni güvenlik tehdit ve zafiyetleri ortaya çıkmıştır. 2008 yılında 22 kamu hizmeti vererek hayatımıza giren e-devlet hizmetinin kullanıcısı sayısı bugün 40 milyona yaklaşmış durumdadır ve verilen hizmet 460 kuruma 3 binin üzerinde hizmete ulaşmıştır. Bu sayılar kamu kurumlarının da hizmetlerinin büyük kısmını internet veya ethernet ağına çevirdiğinin basit bir göstergesidir.

Bütün bu gelişmelerin sonucunda teknolojinin bu faydalarının devamlılığının sağlanması, sistemlerde bulunan verilerin güvenliği ihtiyaçları hayatımıza siber güvenlik, siber saldırı, siber savaş gibi güvenlik unsurlarını içeren kavramların girmesini sağlamıştır. Siber uzayın böylesine yaygınlaşması, büyümesi, güvenlik boyutunun ortaya çıkması bizleri siber uzayın güvenlik üzerine etkilerinin ne olduğu konusu üzerinde düşünmeye ve tartışmaya sevk etmiştir.

Siber güvenlik ve siber savaş kavramlarının göründüğü kadar bir konvansiyonel savaş boyutunda tehdit olmadığını savunan yaklaşımlar olsa da en temel yaklaşım siber güvenliğin gerçek ve ciddi bir ulusal güvenlik konusu olarak ele alınması gerektiğidir. Çalışmamızda siber güvenlik kavramının milli güvenlik açısından öneminin, siber uzay ve reel dünyaya etkisi boyutunda literatür taraması ile dünyada yaşanmış siber saldırı, siber terörizm ve siber savaş örnekleri ile ele alınacaktır.

Siber uzayın ve içerisinde yer alan kavramların sürekli ve hızla gelişip büyümesi yanında yeni güvenlik tehditlerini de getirmektedir. Bu çalışma ile bu gelişmelerin takip edilmesi gerekliliği ve öneminin üzerinde durularak milli güvenliğin siber güvenlik bağlamında da düzenli olarak değerlendirmeye tabi tutulması gerektiği vurgusu ile çalışman konusunun en temel sınırlılığı olan bireysel bilinçlendirme faaliyetine katkı sağlanmış olacaktır.

Siber güvenlik alanında yürütülen faaliyetlerin diğer bir sınırlılığı ise bireysel unsurların milli güvenlik boyutuna ulaşacak zafiyetlere sebep olabilecek olması ve bu konuda bilinçli personel kitlesinin sınırlı olmasıdır. İnternet ve Telekominikasyon Ajansı'nın hazırladığı Küresel Siber Güvenlik İndeksinde alanda olgunlaşan ülkeler arasında gösterilen Türkiye küresel sıralamada daha az gelişmiş birçok ülkenin gerisinde kalarak 43. sırada yer almıştır. Buradan hareketle Türkiye'nin siber güvenlik alanında oldukça ciddi adımlar atması gerektiğini söyleyebiliriz.

Alınan ve alınması gereken tedbirlerin de incelendiği bu çalışma, siber güvenlik alanında yer alan birçok konunun teknik bilgi içermesi ve sonucunun tahmin edilebilir olmaması sebebiyle, kavramların açıklanması ve örneklenmesi sonrasında güvenlik alanına etkisi çerçevesinde incelenmesi şeklinde ilerleyecek ve siber tehditlerin Milli Güvenlik için göz ardı edilmeyecek boyuta ve öneme ulaştığı üzerinde durulacaktır.

2. SİBER UZAYIN GÜVENLİK BİLEŞENLERİ

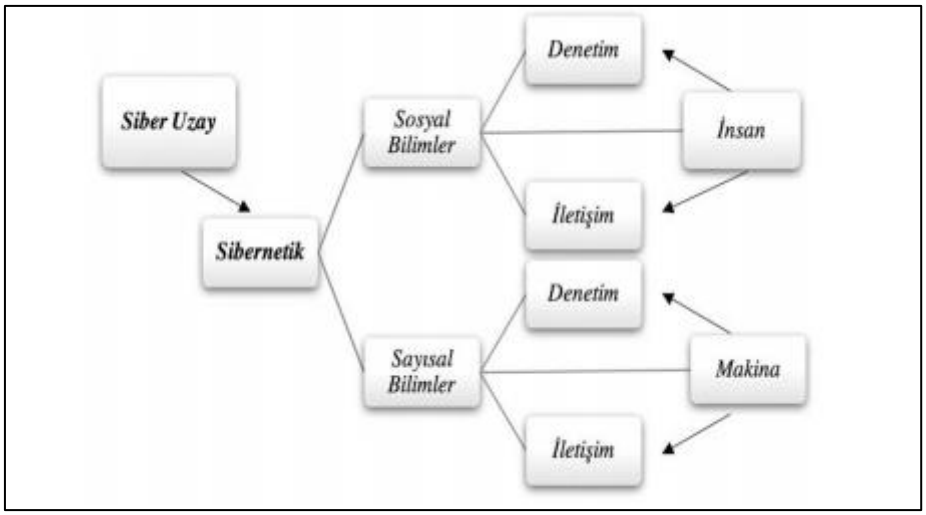
Siber güvenlik kavramının incelenmesi öncesinde siber uzayda sıkça yer alan kavramların açıklanması konunun gelişim sürecine ve hayatımızdaki yeri ve önemini anlama konusunda faydalı olacaktır. Her geçen gün büyüyen, bünyesine yeni kavramlar ekleyen siber terimlerin tanımlamasına ve isimlendirilmesine, sibernetiğin teknoloji gelişimine paralel olarak büyümesi sebebiyle, teknolojiye öncülük eden ülkeler paralelinde siber uzayın gelişme ve kavramlaştırılmasına yabancı kaynaklar öncülük etmektedir.

2.1. Sibernetik – Güdüm Bilimi'nin Doğuşu

Son yıllarda hızlı ilerleyen teknolojik gelişmeler sonucu karşımıza daha sık çıkan ve günlük hayatta sıkça yer alan bu bilim dalı yaşantımızın her alanında eğitim, sağlık, iletişim ve güvenlik gibi birçok sektörde kullanılmaya başlanmış olan sibernetik terimi, güncel anlamına matematikçi ve felsefeci Norbert Weiner tarafından 1948 yılında yazdığı kitapla kavuşmuş olsa da ilk olarak matematik ve fizikçi André Marie Amperé tarafından 1834 yılında kullanılmıştır. Türkçe karşılığı, TDK'ya göre "Canlılarda ve makinelerde kontrol, iletişim ve işleyişi inceleyen bilim." olarak tanımlanan "Güdüm Bilimi" şeklinde kullanılmaktadır.[1]

"Sibernetik canlılarda kendi kendini düzenleyen makineler arasındaki çalışma benzerliklerini araştırır. Bu bakımdan "organize varlıkların davranış bilimi" şeklinde de düşünülebilir." (Kaban, 1994, s. 219-226) İnsana özgü sinir sistemini makinelere uygulamaya çalışarak dış müdahaleye gerek olmadan öz gelişimle insan müdahalesi olmadan da işlem yürütebilen tasarımlar yapılması için çalışmalar yürüten bilim dalıdır ve teknolojik gelişmelerin temelini oluşturmaktadır. Dünyada her geçen gün artış gösteren yapay zeka çalışmaları bunun bir sonucudur.

[1] https://sozluk.gov.tr/?kelime=g%C3%BCd%C3%BCm%20bilimi Erişim Tarihi: 11.11.2019



Şekil 2.1. Sibernetiğin, siber uzay içerisinde bilimsel olarak kurulumu (Vinnakota, 2013)

Sibernetik sistemlerin başlangıcı konusunda farklı isimler öne sürülse de yaşadığı dönem itibari ile bu işin öncüsü "Ismail Ebul-Iz Bin Razzaz El-Cezeri"dir. El-Cezeri, rakiplerinden tam 600 yıl önce sibernetiğin ilkelerini bilim dünyasına sunan ilk kişiydi.[2] Sibernetik ve robot biliminde çalışmalar yapan El Cezerî, "Mekanik Hareketlerden Mühendislikte Faydalanmayı İçeren Kitap" (El Câmi-u'l Beyn'el İlmî ve ElAmelî'en Nâfi fî Sınâ'ati'l Hiyel) eserinde çok sayıda cihazın yararlanma olanaklarını, kullanım esaslarını ve çizimlerini kaleme almıştır. Günün mekanik ve teknik imkânları doğrultusunda çizimleri yapılan bu tasarım ürünü makineler sibernetiğin ilk kullanım örneği olarak adlandırılabilir.

Şekil 2.2. Tavus kuşlu abdest alma makinesi ((Ertürk & Yayan, 2012)

[2] Çırak, B., & Yörük, A. (2016). Mekatronik biliminin öncüsü İsmail El-Cezeri. *Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (4), 175-194.

Genel itibariyle sibernetik; insan-makine arasında etkileşim kuran, bütün bilim dalları için ortak olan iletişim-kontrol süreçlerini içine alan, geribeslem için pratikler yaratan mekanik sistem olarak tanımlanabilir.[3] (Sezgin & Talaz, 2016)

Bu bağlamda Sibernetik'in insan ve makine aynı zamanda makineler arası etkileşim oluşturmasının ve disiplin geliştirme çabasının adeta bir kontrol mekanizması görevi üstlenerek birçok bilime katkı sunduğunu söylemek mümkündür.

2.2. Siber Uzay Boyutu

Teknolojinin gelişmesi ile bireylerin etkileşim imkânlarının kolaylaşması ve hızlı hale gelmesi insanların iletişime olan bağlılığını artırmıştır. Günümüz toplumunda artan internet kullanımı ile de farklı kesimlerin ağda birbirleriyle iletişim kurmasını sağlanmaktadır. Siber uzay olarak adlandırılan, önemi ve boyutu gün geçtikçe artan bu ortamda bilişim sistemleri ağda birbiriyle bağlı olarak faaliyet göstermektedir.

Siber uzay kavramı 1984 yılında "Neuromancer" adlı romanda William Gibson'ın tarafından kullanımı sorasında yaygınlaşmıştır. Gibson Siber Uzay'ı şu şekilde tanımlamıştır:

> Matematiksel kavramların öğretildiği çocuklar tarafından, her milletten milyarlarca yasal operatörün deneyimlediği, her gün yaşanan içgüdüsel ve tepkisel bir sanrı. İnsan sistemindeki tüm bilgisayar kümelerinden oluşturulmuş verilerin grafiksel gösterimi. Düşünülemez bir karmaşıklık. Belleğin mekânsızlığında, verilerin kümelerinde ve takımyıldızlarında gezinen ışık çizgileri (Gibson, 2016:69-70).

ABD Genelkurmay Başkanlığı tarafından yapılan tanıma göre siber uzay (Cyberspace) "İnternet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler dâhil olmak üzere, birbirine bağlı bilgi teknolojileri altyapıları ağlarını ve bilgi verenleri içeren küresel alandır."[4]

Türkçe'de siber âlem, sanal ortam veya sanal dünya gibi farklı şekillerde kullanılan siber uzay kavramı sanal yaşam alanı olarak da adlandırabileceğimiz yapay bir ortamdır. Fakat siber uzayı ABD tarafından 1969 yılında geliştirilen Advanced Research Projects Agency Network (ARPANET) projesine sayesinde ilk bilgi transferi gerçekleştirilme ile başlayıp günümüzde şeklini alan "internet" kavramına indirgeyen yaklaşımlar isabetli değildir. Binlerce bağımsız ağdan oluşan internet, bu sanal alanın yalnızca bir parçasını oluşturur. (Nye, 2014, s. 3-5) Siber-uzay interneti kapsamakla birlikte, enformasyon sistemleri,

[3] Sezgin, M., & Talaz, L. (2016). Bilişim Devrimi, Sibernetik İletişim ve Stratejik Halkla İlişkiler. *Karabük Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *6*(2), 559-571.
[4] https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf, Erişim tarihi: 18 Nisan 2019.

fiziksel, yazılımsal bilgi sitemleri parçaları ve bu unsurlarla ilgili kişiler ve ağlar arasındaki etkileşimin tamamını da içermektedir.

Dünyaya yayılmış bilişim sistemlerinden ve sistemleri birbirine bağlayan ağların oluşturduğu ortam olarak önümüze çıkan siber uzayın katılımcısı günbegün artmaktadır. Aşağıda yer alan We are Social kuruluşu tarafından açıklanan internet kullanım rakamları siber uzayın ne kadar büyüdüğünü gösteren en önemli göstergelerdendir.

Şekil 2.3. Global digital 2019 reports, https://wearesocial.com/global-digital-report-2019

Kasapoğlu'na göre siber uzay "…verilerin bilgisayarlar ve diğer elektronik cihazlar ile depolanabildiği, değiştirilebildiği ve iletilebildiği ağ tabanlı sistemler ve bu sistemler ile bağlantılı fiziksel altyapı… "[5] şeklinde betimlenebilir. Gelişen fiziksel altyapının bir sonucu olarak günümüzde 7 milyar insanın 5 milyarı mobile telefon kullanmakta, 4 milyar insan internet kullanmakta ve bu kişilerin 3.5 milyarı sosyal medya kullanmaktadır.

Sınırsız bilgiyi barındırması ve iletişim ağıyla paylaşımını kolaylaştırması sebebiyle, büyük bir öneme sahip olan siber uzaya ait yetenekler sahip olunması avantaj olan unsurlardan çok sahip olunması zorunlu kimliğine bürünmüştür ve hayat için olmazsa olmaz bir unsur haline gelmiştir. Bu sebeple hayatın temel unsurlarından olan bu sistemler bütünün saldırılardan korunması ve devamlılığının sağlanması sadece bireysel değil toplum için de elzemdir.

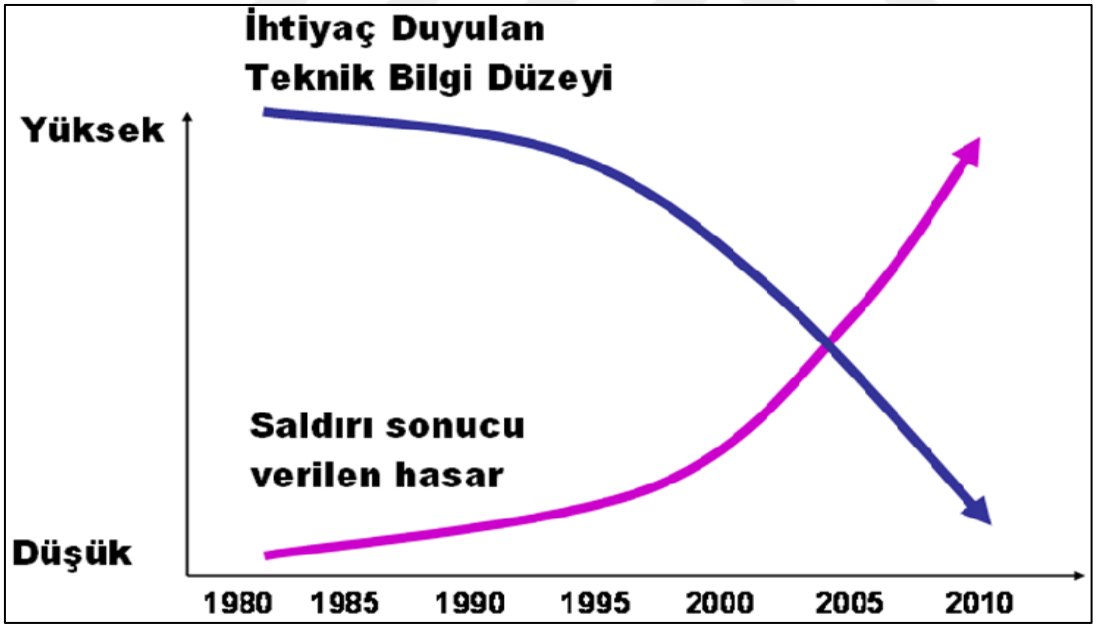
[5] Kasapoğlu, C. (2017). Siber Güvenlik: Beşinci Boyutu Anlamak.

2.3. Siber Saldırı

Bilişim sistemlerinde yaşanan gelişimler, internet altyapısının her geçen gün büyümesi siber uzay ile toplumsal hayatta yeni bir boyut açmış ve yaşamın bir parçası haline gelmiştir. İçeriğinde sürekli artan bilgiyi bulunduran ve büyüyen bu boyut hırsızlığın, dolandırıcılığın, casusluğun, şiddetin, istismarın da hedefi-alanı olmuş ve siber saldırı olarak literatüre girmiştir.

Siber uzayda, bilgisayar sistemlerinde gerçekleştirilen birtakım yöntemler ile veri çalma, casusluk, maddi kazanç sağlama vb. amaçlarla hedef kurum, şirket veya kişilerin bilgi sistemlerine veya iletişim altyapılarına yapılan genel itibariyle planlı ve koordineli yapılan saldırılara "siber saldırı" denir.

2016-2019 Ulusal Siber Güvenlik Stratejisi[6] (2016: 7)'ye göre siber saldırı, ulusal siber uzayda bulunan bilgi ve iletişim teknolojilerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi veya sistemler tarafından kasıtlı olarak yapılan işlemlerdir.



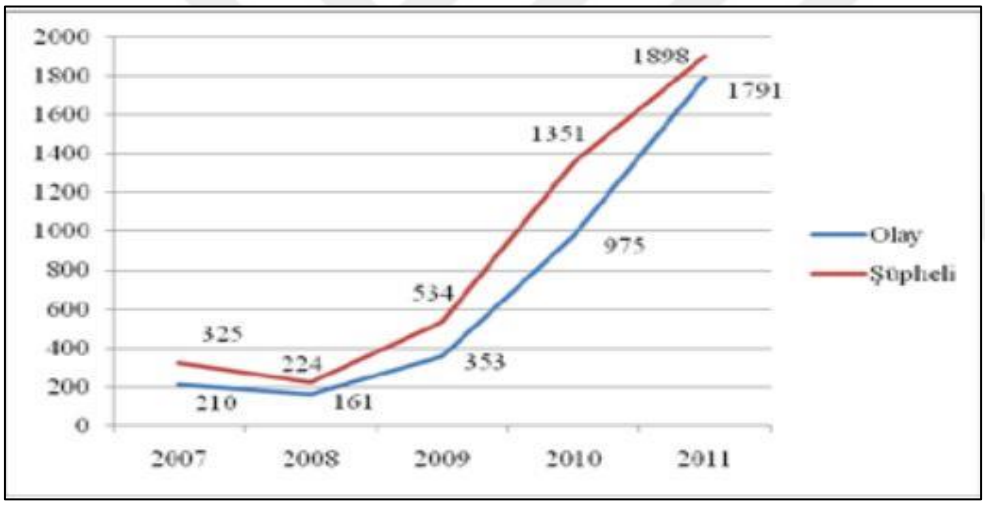
Grafik 2.1. Saldırı ve bilgi düzeyi grafiği (Çeliktaş, 2016)

Fiziksel suç ve saldırılardan farklı olarak siber saldırıcı için teknik bilgi gerekmektedir. Fakat gelişmelerin olumsuz bir yönü olarak da görebileceğimiz, ihtiyaç duyulan teknik bilginin her

[6] Ulaştırma ve Altyapı Bakanlığı - 2016-2019 Ulusal Siber Güvenlik Stratejisi https://www.uab.gov.tr/siber-guvenlik Erişim Tarihi:12/11/2019

geçen gün azalması bilinçsiz kullanıcılar tarafından da saldırı gerçekleştirilmesine olanak sağlamaktadır. Siber ortamda bir saldırı yapmak için ihtiyaç duyulan enstrümanlar çoğu zaman bir ağ bağlantısı ve bilgisayardan ibaret olacak kadar ucuz ve erişimi kolay olabilirken bu mağdur taraf açısından yüksek bedeller ortaya çıkarmaktadır. (Gürkaynak & İren, 2011) Grafik 2.1'de bu dengenin ters orantıya dönüştüğünü rahatlıkla görebilmekteyiz.

İlk siber saldırı Kasım 1988 de şu an MIT'de profesörlük yapan ve İnternet'in ne kadar büyük olduğunu ölçmeye çalıştığını söyleyen Robert Tappan Morris tarafından yazılan ve sonrasında Morris Solucanı olarak adlandırılan yazılım ile yapılmıştır. ABD'nin bilgisayar dolandırıcılığı ve kötüye kullanımı yasası altında mahkûm olan ilk kişi olmuştur.[7] Bütün bu teknoloik ve bilişimsel gelişmelere paralel olarak siber saldırılar ve siber saldırı türleri de her geçen gün çeşitlenmekte ve artmaktadır. Artan saldırılar siber güvenlik alanının önemini de ortaya koymaktadır.



Grafik 2.2. 2007-2011 yıllarında bilişim sistemlerine karşı işlenen suçlara ilişkin olay ve şüpheli sayıları, Kaynak: (EGM, 2011)

Siber uzayla ilgili uluslararası kurallara yönelik en kapsamlı çalışma olarak kabul edilen[8] Tallinn El Kitabı'nda siber saldırı; savunmaya veya saldırıya yönelik olmasına bakılmaksızın, insanların yaralanmasına ya da ölmesine, nesnelerin yok olmasına ya da zarar görmesine neden olan siber eylemler olarak tanımlanmıştır.[9]

[7] https://www.nato.int/docu/review/2013/Cyber/timeline/TR/index.htm Erişim Tarihi: 02 Mayıs 2019
[8]https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku
[9] Michael N. Schmitt, ***Tallinn Manual on the International Law Applicable to Cyber Warfare,*** Cambridge University Press, 2013, s.92.

Tıpkı fiziksel savaş veya espiyonaj gibi siber saldırılar da bireysel olmanın dışında ülkelerinde faaliyet alanına ve kontrolüne girmiştir. Saldırı kadar saldırılara karşı koyabilmek içinde önemli olan siber saldırı gücü ülkelerin Siber Saldırı Güçleri Sıralaması[10] aşağıdaki tabloda gösterilmiştir.

Sıra Nu.	Ülke	Toplam Siber Saldırı Gücü	Siber Saldırı Gücü
1	ABD	26,85	**8,95**
2	Çin	22,49	**7,5**
3	Japonya	17,37	**5,79**
4	Almanya	16,2	**5,4**
5	Rusya	13,97	**4,66**
6	İngiltere	13,77	**4,59**
7	Güney Kore	12,87	**4,29**
8	Fransa	12,52	**4,17**
9	Kanada	12,33	**4,11**
10	İtalya	11,34	**3,78**
11	Brezilya	10,37	**3,46**
12	Hindistan	9,02	**3**
13	İsrail	8,62	**2,87**
14	**Türkiye**	6,97	**2,32**
15	İran	2,45	**0,82**
16	Kuzey Kore	2,45	**0,82**

Tablo 2.1. Ülkelerin siber saldırı güçleri (Çeliktaş, 2016)

Bu yönüyle günlük hayatın bir parçası haline gelen siber uzayın unsurları olan internet ve teknolojiyi tehdit eden siber saldırının da çeşitli yol ve yöntemleri gelişmiştir. Saldırılarda

[10]https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks +originate+-++2015.pdf Erişim Tarihi:12/11/2019

kullanılan bu siber silahlar da saldırının mahiyeti amacı ve hedefine göre değişmekte ve gelişmektedir.

2.3.1. Siber Silahların Gelişimi ve Çeşitliliği

Bilgi sistemlerini ve iletişim altyapılarını hedef alan materyallerin kişi ve kurumlar üzerindeki tahrip edici etkisi gün geçtikçe artmakta, yapılan saldırıların yöntemleri ve bu saldırılarda kullanılan yöntemler-silahlar da çeşitlenmektedir.

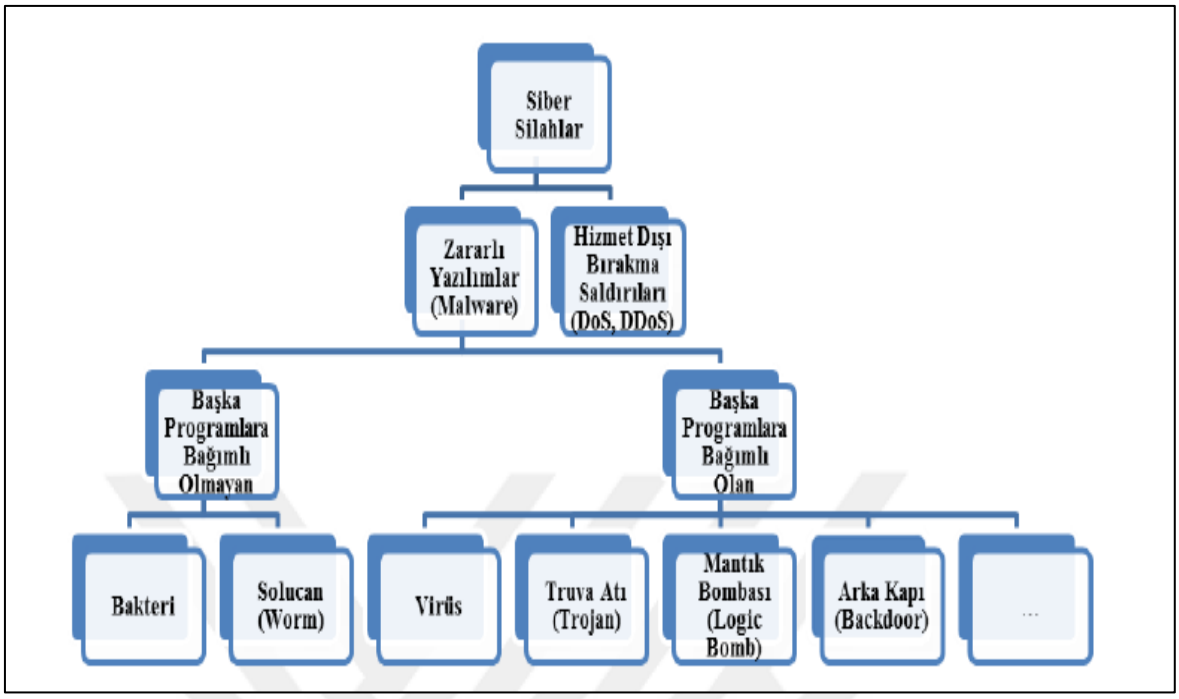
Savunma ya da saldırı amaçlı kullanılan her türlü araca silah denilmektedir.[11] Tanımdan da anlaşılacağı üzere materyalin ne olduğu değil ne için hangi amaca matuf olarak kullanıldığı silah olup olmadığını belirleyen unsurdur. Kısaca yapılacak bir siber saldırıda kullanılan siber uzay araçlarına siber silah denilebilir. Siber silah dar kapsamda sadece saldırı için tasarım sonucu yazılımlar ile yapılmış olabileceği gibi geniş kapsamda amaca yönelik kullanım ile siber ortam araçlarının herhangi birini kullanarak sistem açıklarının ortaya çıkması veya tespiti ile de yapılabilmektedir.

Tallinn El Kitabı'nda siber savaş araçlarını tanımlanırken, siber saldırı amacıyla planlanan ya da kullanılan her türlü siber araç-teçhizat, mekanizma ve donanımdan bahseder. Siber etkinliklerin, bir saldırı, insan öldürme, yaralama veya siber ortamda tahrip etme veya yok etmenin bir aracı olarak tasarlanmış veya kullanılmış siber savaş araçlarını da siber silah olarak kabul edilir.[12]

Konvansiyonel silahlar ile kıyaslandığında siber silahlar, üretilmeleri için daha az zamana ve daha az paraya ihtiyaç duymaktadır ve hedef üzerinde uygulanması da daha kolaydır. Bu özellikleri ile siber silahlar, devlet dışı aktörler tarafından çok daha yaygın şekilde kullanılmaktadır. Ayrıca, konvansiyonel silahların aksine, siber silahlar düşük maliyetler ile yeniden üretilebilmekte, bilgi ve iletişim teknolojilerine çok kısa sürede yayılabilmekte ve fiziksel bir risk olmadan uzun süre saklanabilmektedir.

Az maliyet ve daha büyük edinim elde etme imkânı sebebiyle siber silahlara yönelim suçlular terör örgütleri için kolay yol olarak görülmekte ve tercih edilmektedir. (Avşar, 2017) Asimetrik savaş olarak da nitelendirilen siber savaşta devletler de bu yöntemlere başvurarak özelikle istihbarat elde etmek için çeşitli siber silahlar kullanmışlardır. Başlıca siber silah türleri ağıdaki tabloda belirtilmiştir.

[11] http://www.tdk.gov.tr/index.php?option=com_gts&kelime=S%C4%B0LAH Erişim Tarihi: 03.05.2019
[12] Michael Schmitt, *Tallinn Manuel on the International Law Applicable to Cyberwarfare*, 2013, Rule 41, s.141-142.



Tablo 2.2. Siber silah türleri (Çifçi, 2013)

2.3.1.1. Virüslerin yapısı ve çalışma prensibi

Siber saldırı denilince akla ilk gelen unsur olan virüsler siber uzayda sıkça karşılaştığımız bir terim ve her ne kadar yanlış bir kullanım olsa da genellikle kapsayıcı şekilde bütün zararlı yazılımlar için kullanılmaktadır.

Virüsler temel olarak diğer dosyalara bulaşarak sistemi kullanılamaz hale getirmek için tasarlanan zararlı yazılım türünü ifade etmektedir. Virüsler genel itibari ile uygulama dosyaları olarak oluşturulan ve kullanıcı tarafından programın çalıştırılması ya da doğrudan sistem tarafından başlatılması sonucu devreye girerek yayılmaya başlamaktadırlar.

Virüsler kısa bir mesaj göstermek için yazılmış olabileceği gibi günümüzde bilgisayarlara fiziksel zarar verecek seviyede tehlikeli olabilmektedirler. Bir kere tespiti yapılan virüsün aynı işlevi tekrar görmesi çok zor olduğundan virüsler de giderek gelişmektedir. Virüslerin ne kadar tehlikeli bir silah olabileceği, kendisini geliştirmekte olan yazılımcının niyetine ve zekâsına bağlıdır.[13]

Virüsler sıklıkla elektronik posta, harici depolama araçları ile yapılan dosya transferlerinde ve internet aracılığı ile yapılan dosya indirmeleri sırasında bulaşmaktadır. İlk kişisel bilgisayar virüsü BRAIN 1986 yılına Pakistanlı Basit ve Amjad Farooq ALVİ tarafından

[13] Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi. Keleştemur, S. A. (2018),

korsan yazılımı engellemek amacıyla yazılmış olsa da günümüzde masum amaçlar için kullanılmamaktadır.

Bütün verilerin bilişim sistemleri üzerinde olduğu günümüzde siteme kötü niyetlerle yerleştirilmiş bir virüs bulaşması fiziksel dünyaya uyarladığımızda kasanızın anahtarının kopyasını başka birinde daha olması anlamına gelmesidir.

2.3.1.2. Truva atlarının(trojan) türleri ve çalışma prensibi

Bilişim sistemlerini kullanılamaz hale getiren zararlı yazılımlar, etkisini yalnızca dosyalar arası yayılma yoluyla göstermezler. Dahil oldukları sistemlerde hassas verileri hedef alan kullanıcı yetkilerini ele geçirme imkanı sunan yazılımlar da mevcuttur. Başlıca Trojan veya tam adıyla Trojan Horse olarak bilinen Truva atı genellikle güvenli bir program olarak maskelenen bilgisayara giriş yaptıktan veya sosyal mühendislik faaliyetleri ile yüklendikten sonra sisteme erişim sağlayarak işlemlerini takip edilebilmesine, hassas verilerin ele geçirilmesine ve sisteme arka kapı erişimi oluşturmaya olanak sağlayan zararlı kodlar içeren bir yazılımdır.

Truva Atı terimi Troya Efsanesinde geçen Truva Atı hadisesinden gelmektedir, zararsız görünmesine rağmen tehlikeli olmasını temsil etmektedir.[14]

Virüslerin aksine, Truva atları kendilerini çoğaltmazlar, ancak aynı derecede yıkıcı olabilirler. Sitemde oluşturdukları açık sayesinde zararlı programların ve kişilerin siteme girmesine imkân tanırlar. Farklı türlerde ve farklı kullanım alanları için yazılmış Truva atları bulunmaktadır.

- ❖ Uzaktan Erişim Truva Atları
- ❖ Veri Gönderen Truva Atları
- ❖ Yıkıcı Truva Atları
- ❖ Proxy Truva atları
- ❖ FTP Truva atları
- ❖ Güvenlik yazılımı engelleyici Truva atları
- ❖ Hizmet reddi saldırısı (DoS) Truva atları

[14] https://www.britannica.com/topic/Trojan-horse Erişim tarihi: 12/11/2019

Buradan hareketle, teknik anlamda zayıf olan sistemlerin Truva atlarına kapı araladığını söylemek mümkündür. Teknik açıklardan sisteme dahil olabilen Truva atları, sistem kontrolünü hızla ve kolaylıkla kullanıcının elinden alabilecek veya sitem üzerinde açık kapılar bırakarak saldırıya elverişli hale getirebilmektedir. Truva atı bulaşmış bir kurum bilgisayarı kurumsal bütün bilgi ve belgelerin içeriklerinin dışarıya açılmasına imkan ve olanak sağlayabilir.

2.3.1.3. Solucanların yapısı ve çalışma prensibi

Saldırganların zarar vermek dışında amaçlarına yönelik olarak geliştirdikleri, sistem kullanıcılarının kişisel veya kurumsal işlemleri takip etmek için kullandıkları tehlikeli yazılımlardan biri olan Solucanlar, ağ üzerinden hızla çoğalarak hedef kitleye kolayca ulaşabilmektedirler.

Solucanlar bilgisayarlarda ya da ağlarda kullanıcı eylemine ihtiyaç duymadan kendini çoğaltan bağımsız kötü amaçlı bilgisayar programlarıdır. Solucanlar yayılmak için bir taşıyıcı programa veya dosyaya gereksinim duymadıklarından, sisteminizde bir tünel açabilir ve saldırganın uzaktan bilgisayarınızın denetimini eline geçirmesini sağlayabilir.[15]

Solucanlar ise genellikle sisteme zarar vermez kullanıcı işlemlerini takip etmek için kullanılır. Truva atları ise bilgisayara girdiği programın aktifleşmesi ile harekete geçebilir ve bilgisayarın işletim sistemine zarar vermek için tasarlanmıştır.

Sistemlerdeki açıklardan yararlanarak sürekli kendini kopyalaması yönüyle solucanlar virüslere benzese de virüslerin çalışması için aktif bir program gerekirken solucanlar yardım olmadan çoğalabilen kötü amaçlı programlardır. Genellikle ağ bağlantıları üzerinden kopyasını oluşturarak yayılır.[16]

Dosyaların işlevini sürdürdüğü; fakat kendi kendine kopya yoluyla çoğaldığı durumlar, solucanlar tarafından sistemin başkasının takibine sunulduğunu belirten alarm durumlarıdır. Devlet kurumlarında bir bilgisayar ağına bulaşan bir solucanın ağ hareketlerini izlemeye imkân vermesi kişisel ve kurumsal işlemlerin gizliliğini ihlaline imkân sağlayacaktır. Bu kurumun bulunduğu konum ise bu ihlalin ne kadar büyük ve etkili olacağını belirleyen unsur olacaktır. İlerleyen bölümlerde yer alacak olan Stuxnet olayı bu konuya en iyi örneği teşkil etmektedir.

[15] https://www.cisco.com/c/en/us/about/security-center/virus-differences.html Erişim Tarihi: 14.05.19
[16] https://www.kaspersky.co.uk/resource-center/threats/viruses-worms Erişim Tarihi 12/11/2019

2.3.1.4. Mantık bombalarının kullanım şekli

Saldırganların da sürekli kendi silahlarını geliştirme çabası içinde olduğu bir gerçektir. Bu konuda teknik bilgi isteyecek şekilde tasarlanmış saldırı silahlarının olduğunu, bilişim ağlarının kullanımını kolaylaştıran programlar içinde yuvalanarak kullanıcıların dosyalarını tahrip edeceği zamana kadar sistem tarafından sorunsuz olarak görülen, yıkıcı bir etkiye sahip olduğu fark edilemeyen saldırı silahı tasarımlarının da geliştirildiği bilinmektedir.

Farklı değişkenlere göre programlanan bir olayın meydana gelme anına kadar veya önceden belirlenmiş bir zamana, bir gecikme süresine kadar aktif olmayan, hareketsiz kalan bir uygulamanın veya işletim sisteminin yazılımında yer alan kötü amaçlı kod parçaları veya programlardır. Programlanan olayın olması halinde ise virüs veya truva atı gibi davranırlar, verileri yeniden biçimlendirme, değiştirme, silme veya bozma gibi eylemler gerçekleştirebilirler. (Sharma, 2017)

Belirli bir bilgisayar işlemine veya zamana ayarlanmış olan virüslerin mantık bombaları oldukları kabul edilir. Genel itibari ile kötü amaçlı olan ve sabotaj eylemleri için programlanan mantık bombalarının, deneme sürümlerinin denetimi ve kontrolü içinde kullanıldığı durumlar mevcuttur. Tüketici ücretsiz deneme sürümü süresi sonunda satın almazsa, yazılmış kodlar devreye girerek programı devre dışı bırakır.[17]

Mantık bombalarının harekete geçmesi belirli şartlara bağlanmıştır. Belirli bir koşula bağlanması sebebiyle bu zararlı yazılımlar özel hedeflere yönelmektedir. Saldırgan ne amaçladığını bilerek amacına uygun koşulun gerçekleşmesi anına kadar zararlı kodların pasif kalmasını sağlayarak uygun zamanda aktifleştirip veriyi-bilgiyi ele geçirmektedir. Bu yönüyle casus yazılıma benzerlik göstermektedir.

2.3.1.5. Casus yazılımların kullanım şekli

Teknolojik imkânların ilerlemesiyle kişisel verileri temin etmek, kişileri izlemek, takip etmek amacıyla oluşturulan casus yazılımlar bireysel amaçlar için dahi kullanılmaya ve yazılımsal olarak geliştirilmeye başlanmış ve günümüzde kolaylıkla ulaşılabilir hale gelmişlerdir.

Casus yazılım, kullanıcının bilgisi olmadan siber casusluk faaliyetleri amacıyla yüklenmiş olan geliştirici tarafından tanımlanan işlemleri gerçekleştiren zararlı yazılımlardır. Kullanıcı izni olmadan indirilen her türlü yazılım kişisel bilgilerin güvenliği sebebiyle casus yazılım

[17] https://searchsecurity.techtarget.com/definition/logic-bomb Erişim Tarihi:12/11/2019

olarak sınıflandırılabilir fakat nispeten zararsız sebeplerle, genellikle bedava deneme sürümlerin yanında, kurulan çeşitli uygulama sözleşmelerinin okunmadan kabul edilmesi ve kurulum aşamalarının hızlı atlanması sırasında son kullanıcı rızasıyla bilgisayarlara kurulmaktadır.

Kurulan casus yazılımlar kullanıcı adı, şifre, kredi kartı bilgileri, eposta bilgileri, banka hesap bilgileri, kullanım alışkanlıkları gibi hassas bilgileri kaydedip önceden belirlenmiş hedefler ile paylaşabilir veya mikrofon ve webcam gibi donanımları otomatik olarak aktifleştirerek bilgilerinizi elde edebilirler. [18]

Tuş Dinleyiciler (Keylogger): Genellikle casus yazılım ürünlerinin bir parçası olarak kullanılan Keylogger'lar klavye üzerinden elde edilen bilgilerin dışında günümüz tuş dinleyicileri sadece metin değil, aynı zamanda çektiği ekran görüntüleri ve video kayıtlarını da saldırgana gönderebilmektedir. (Keleştemur A. , 2015)

Keylogger olarak da bilinen tuş dinleyiciler, temel olarak klavye hareketlerini izleyen ve kaydeden programlardır ve sistemden elde ettiği kayıt edilen bilgileri bir dosyaya kaydederek ve periyodik olarak saldırgana gönderilmesi şeklinde çalışmaktadır. Fiziksel donanımlar aracılığıyla da yapılabilen bu işlem maliyeti sebebiyle yazılımsal olarak tercih edilmektedir. Yazılım üzerinden yapılan tuş dinleme işleminde hedef sistemin bir ağa bağlı olması gerekmektedir.

Ayrıca ziyaret edilmek istenen web sitesi yerine, kullanıcıyı sahte olanlarına yönlendirmek için kullanılan casus yazılımlar da mevcuttur. Bu tür yazılımların ilk belirtisi, bağlantı hızlarında düşüş, bilgisayarın yavaşlaması, mobil cihazlarda ise veri kullanımında artış ve pil ömründe azalma olmasıdır. Mobil iletişim altyapısının gelişimi sayesinde internet kullanımının dünya nüfusunun %52 sine ulaştığı[19] günümüzde, mobil cihazlara yönelik de casus yazılımlar geliştirmektedir. Casus zararlı yazılımların amacının karşı bilgisayardan veri temin etmenin ötesinde, karşı bilgisayarı kontrol etme isteğine dönüştüğü durumlarda ise köle bilgisayarlar ortaya çıkmaktadır.

[18] https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html Erişim Tarihi: 12/11/2019

[19] https://wearesocial.com/global-digital-report-2019 Erişim Tarihi: 12/11/2019

2.3.1.6. Köle bilgisayarlar oluşturulması (Boot-net)

Bilişim sistemi kullanıcılarının varlığından ve işlevinden haberdar olmadığı bu saldırı unsuru, casus yazılıma benzemekle birlikte, saldırganın kendine sistem üzerinde yönetici yetkilerini alabilmesi yetilerine sahip zararlı yazılımlardır.

Bilgisayar sisteminin uzaktan kontrol edilmesine olanak verecek şekilde saldırganın kontrolünde olduğu ve kullanıcısının haberi olmaksızın saldırganın amaçlarını yerine getiren bilgisayarlara zombi bilgisayar veya köle bilgisayar denilmektedir. Sisteme gizlice yüklenen zararlı yazılımlar sistemin yapısını bozmadan siber suçluya tüm yönetici haklarını verir. Sistem her zamanki gibi normal olarak çalışır fakat aynı zamanda botnet yöneticisinden aldığı emirleri yerine getirir.

Köle bilgisayarların oluşturduğu botnet, zombi ordusu, köle bilgisayar ordusu yapısının kullanıldığı en yaygın yöntem sunucuya yoğun ve lüzumsuz istekler yaparak bu taleplerle dolan sunucunun işlemleri gerçekleştirememesi şeklinde kullanılmasıdır. Botlar sistemlere zarar vermek yerine, çalışmalarını engellemek ya da sistemi yavaşlatmak amacıyla kullanılmaktadır. (Keleştemur A. , 2015, s. 228). Örneğin bir web sitesine aynı anda yönlendirilerek bu siteyi hizmet veremez hale getirmek için kullanılabilmektedirler.[20]

Bu özellikleriyle köle bilgisayarların saldırganların kendilerini ele vermeden saldırı yapabilmelerine imkân tanıdığını, tespit ve takip edilebilmeyi zorlaştırdığını, hedef sistemin işleyişini zorlaştırdığını ve hatta kullanılamaz hale getirdiğini söylemek yerinde olacaktır. Günümüzde ticareti dahi yapılan yani köle bilgisayarların daha gelişmiş saldırıların ön ayağı olarak kullanıldığı da bilinmektedir.

2.3.1.7. Gelişmiş sürekli tehditler (APT)

Teknolojik gelişmelerin paralelinde suç türleri de bilişim sitemleri üzerine yönelmiştir ve geliştirilen silahlar amaçlara göre şekillenmekle birlikte bu yazılımların çok yönlü ve koordineli kullanıldığı siber silahlar Gelişmiş Sürekli Tehditler (Advanced Persistent Threat) olarak isimlendirilmektedir.

Gelişmiş Sürekli Tehditler (Advanced Persistent Threat) klasik saldırı yöntemlerinden farklı olarak; genel itibariyle ticari ve politik hedefler için profesyonel bir şekilde tek bir yönteme bağlı kalmaksızın hedefe yönelik geliştirilmiş araçlar kullanılan ve sisteme hızlı bir şekilde

[20] https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks Erişim Tarihi: 12/11/2019

girmek ya da sistemi tamamen etkisiz hale getirmek yerine yavaş ve fark edilmeden sızarak sistemde olabildiğince uzun süre kalma şeklinde gerçekleşen saldırı türüdür.[21]

APT saldırısının amacı ağ etkinliğini izlemek ve zarar vermek yerine verileri çalmaktır. APT'ler genellikle bir grup veya devlet desteği ile daha kapsamlı belirli sistemleri, kişileri veya kuruluşları hedef almaktadır. (Bircan, 2012) Gelişmiş siber silahlar söz konusu olduğu için klasik siber savunma yöntemleri ve araçları yetersiz kalmaktadır. Genelin dışında ticaret ve politika dünyasında ulaşılmak istenen hedefe karşı planlı nokta atışı ile yapılan saldırılardır. Saldırıya maruz kalan sistemlerin zararlarının çok büyük seviyelerde olması sebebiyle siber savunma sistemleri saldırı türlerine göre gelişim göstermektedir ve sitem yöneticilerinin bu tarz saldırılara maruz kalmamak adına aldığı tedbirlerin saldırıları zorlaştırması sebebiyle zararlı yazılımlar işletim sistemi seviyesine inmiştir.

2.3.1.8. Kök kullanıcı takımı (Rootkit)

Bilişim sistemini tehdit eden yazılımlara yönelik savunma sistemlerin göstermiş olduğu gelişmeler zararlı kodların fark edilmesini ve devre dışı bırakılmasını engelleyen birtakım yöntemler ortaya çıkarmıştır. Verilere ulaşmaya çalışan yazılımları gizleyen profesyonel bir işleyişe sahiptir bu yöntemler.

Rootkitler, bilişim sistemlerine bulaşmış olan zararlı yazılım vb. unsuların kullanıcıdan gizlenerek tespit edilmesini engellemek için, genel olarak işletim sistemlerinin çekirdek düzeyinde çalışarak, sistemde değişiklikler yapan zararlı yazılım program veya kod parçalarıdır.[22]

> İlk nesil rootkitler, salgırganının yönetici haklarına sahip olabilmek, yönetim uygulamaları ile sistem bilgilerine ulaşabilmek ve bunları gizlemek için geliştirilmiştir. Günümüzde kullanılmakta olan yeni nesil rootkitler ise hedef sisteme sızmış olan diğer zararı yazılımların, sistem yöneticileri tarafından fark edilmeden rahat çalışmalarını sağlamak için kullanılmaktadır (Keleştemur S. , 2018).

Bu sebeple de tespit edilmeleri ve sistemden kaldırılmaları oldukça zordur.

Diğer saldırı yöntemlerinin aksine profesyonel seviyede teknik bilgi gerektiren bu saldırı silahlarının tespiti bireysel olarak yapılamasa da bu ve buna benzer saldır silahları için geliştirilmiş programlar sayesinde güvenlik alınmaktadır.

---

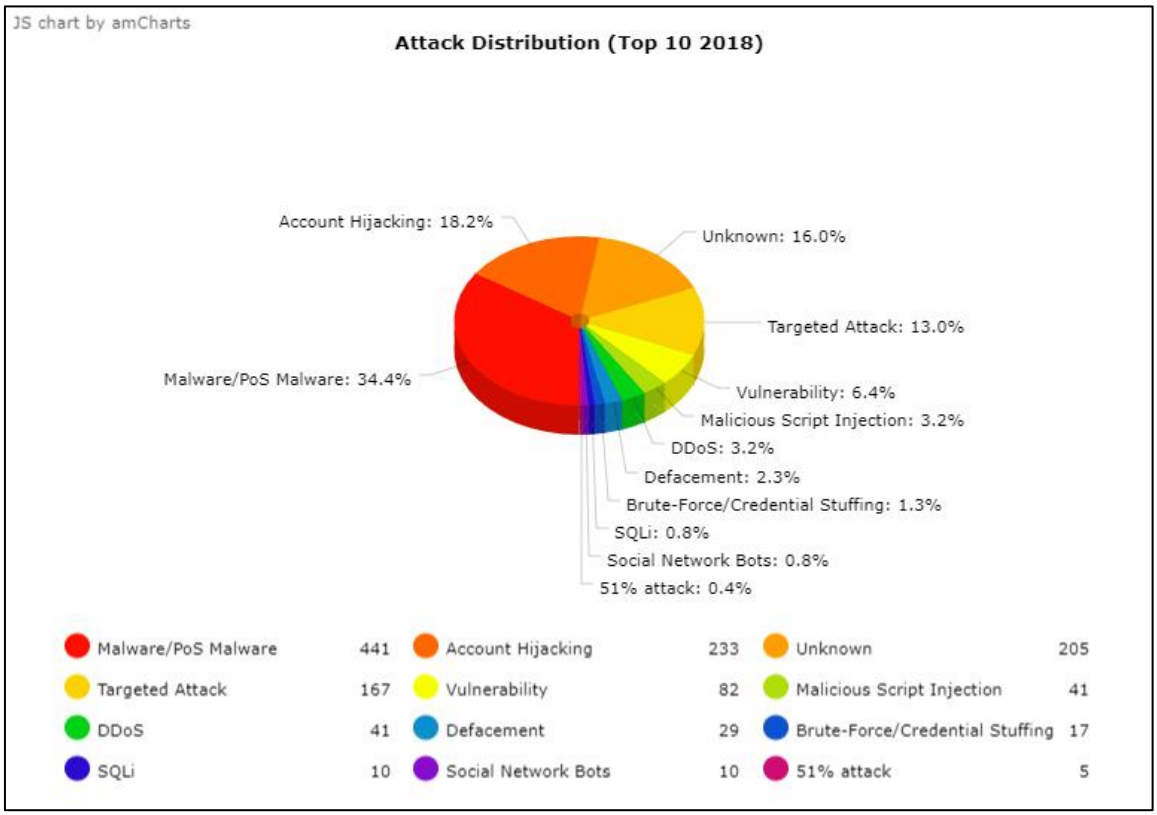
[21] Virvilis, N., & Gritzalis, D. (2013, September). The big four-what we did wrong in advanced persistent threat detection?. In *2013 International Conference on Availability, Reliability and Security* (pp. 248-254).

[22] Canbek, G., & Sağiroğlu, Ş. (2007). KÖTÜCÜL VE CASUS YAZILIMLAR: KAPSAMLI BİR ARAŞTIRMA. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, *22*(1).

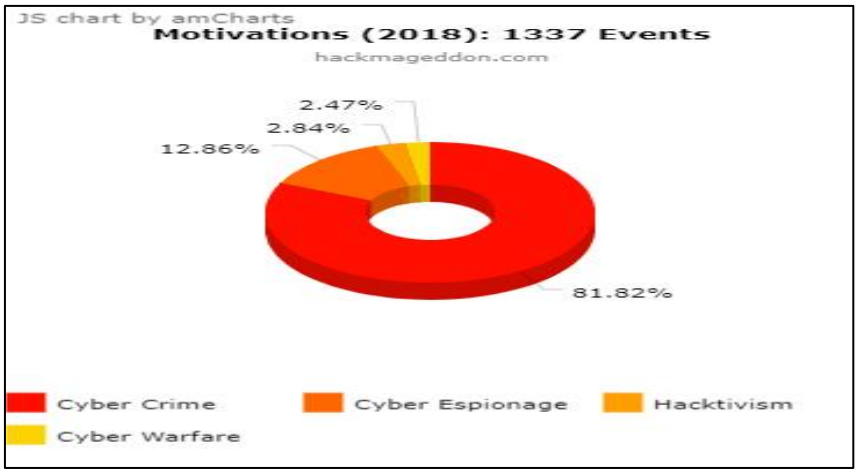
2.3.2. Siber Saldırı Türleri ve Kullanım Yoğunlukları

Siber uzayın internet teknolojisi ile hızla gelişmesi siber saldırı silahları ile birlikte saldırı türlerini de artırmakta ve çeşitlendirmektedir. Siber saldırıların altında yatan motivasyon ve saldırı sebepleri saldırı türlerini değiştirmektedir fakat kimi saldırı türleri her saldırı sebebi için kullanılabilmektedir.

Saldırganların kullandığı yöntemler (Grafik 2.3) ve saldırı güdülerinin ne olduğu (Grafik 2.4) aşağıdaki grafiklerde belirtilmiştir.



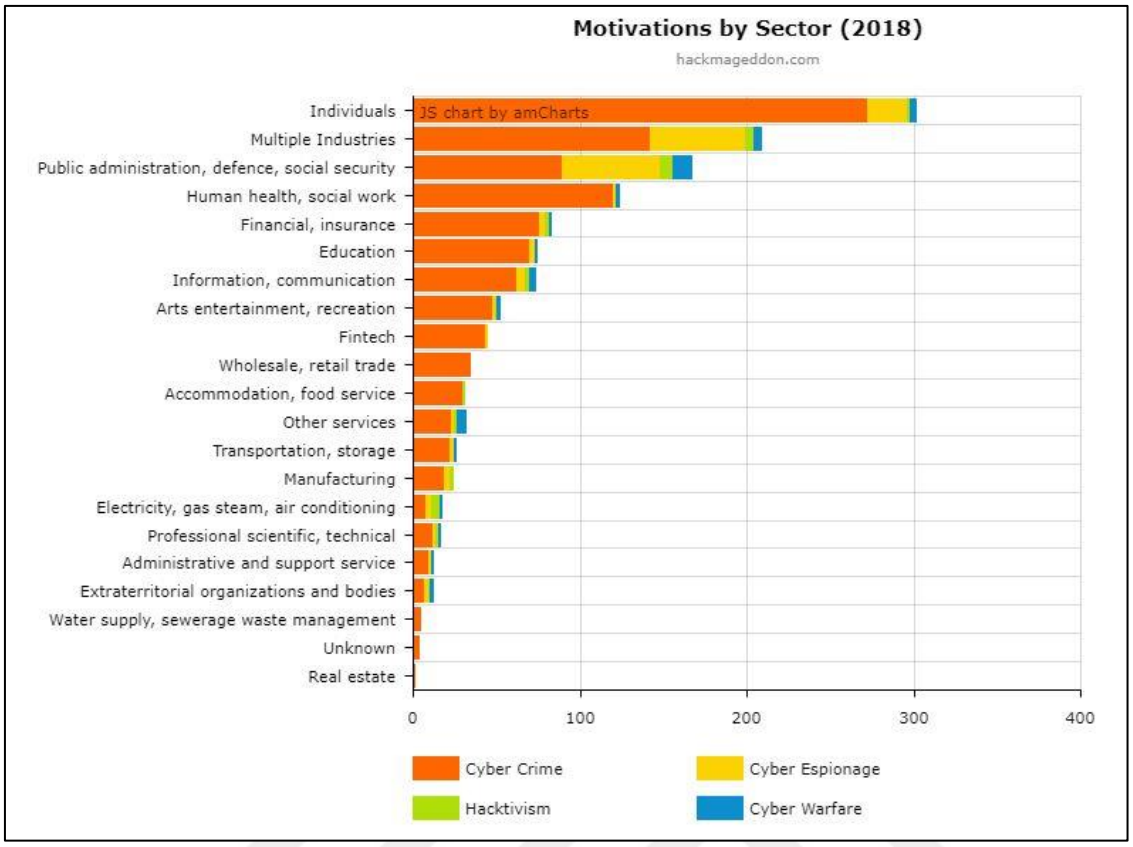
Grafik 2.3. 2018 yılı siber saldırı türlerine göre dağılımı; Kaynak: Passeri, 2019.



Grafik 2.4. Siber saldırıların arkasında yatan sebepler ve güdüler, Kaynak: (Passeri, 2019)

Grafiklerde yer alan saldırı yöntemleri ve saldırı güdülerinin çoğunluğunu siber suç amacıyla zararlı yazılımların kullanımı oluşturmaktadır. Saldırıların türleri farklılık gösterse de en yoğun saldırıların ortak silahı ise zararlı yazılımlar (Malware) yani virüs, solucan, truva atı gibi yazılımlar olmuştur.

Saldırıların işkoluna ve güdüsüne göre dağılım grafiği (Grafik 2.5) incelendiğinde siber suç amacıyla işlenen saldırıların bireysel ve ekonomik hedeflere, siber istihbarat, hackleme ve siber savaş güdüsüyle yapılan saldırıların ise kamu, uluslararası şirketler, güvenlik ve iletişim sektörlerine yöneldiği görülmektedir.



Grafik 2.5. Siber saldırıların işkolu ve güdülere göre durumu, Kaynak: (Passeri, 2019)

Maliyetsiz olması ve ekonomik kazancının yüksek olması sebebiyle artış gösteren siber saldırılar yöneldiği hedefe, saldırının amacına ve kullandığı yöntemlere göre çeşitlenmektedir. Saldırı türlerinde kullanılan silahlar benzer olmakla birlikte silahın kullanım süreci ve buna ulaşma süreci farklılıklar ortaya çıkarmaktadır. En sık kullanılanlarını; [23]

- Sosyal mühendislik
- DOS - DDOS saldırıları (Distributed Denial of Service)
- DNS - İP Aldatmacası
- Arka Kapı (Backdoor-Trapdoor)
- Ağ dinleme Network sniffing)
- Oturum çalma – Yerine geçme (Session Hijacking)

[23] Passeri, P. (2019). *2018: A Year of Cyber Attacks.* https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/

- Phishing (Oltalama)
- SQL Enjeksiyonu

oluşturmaktadır.

2.3.2.1. Sosyal mühendislik saldırısı ve türleri

Siber saldırganların saldırılarının teknik kısımlarını aktif hale getirmek ve sistem üzerinde kullanabilmek için en sık başvurdukları yöntem olan sosyal mühendislik kavramı, siber uzay için, büyük ölçüde insan etkileşimine dayanan insanları manipüle etmeyi içeren, sistem zayıflığını-açığını bulmaktan daha kolay olması sebebiyle sıkça kullanılan saldırı yöntemdir. Elbahadır'a göre sosyal mühendislik, sıradan kullanıcı yetkileriyle, hedef sistem hakkında elde edilemeyecek bilgilerin; insan faktörünün kullanılarak ele geçirilmesidir (Elbahadır, 2012).

Sosyal mühendislik kullanıcıların bilgi eksikliğinden, dalgınlığından faydalanarak veya güvenlerini kazanarak ikna etme, etkileme, aldatma gibi yöntemler ile gizli bilgilerini göndermelerini, kötü amaçlı yazılım bulaştırmasını veya saldırgan için bağlantılar açmasını sağlamak için kullanılan tekniklerdir. Günümüzde neredeyse her tür saldırı belirli noktalarında bir tür sosyal mühendislik içermektedir ve sosyal mühendislik saldırılarının başarılı olması halindeki en muhtemel sonucu ise zararlı yazılım bulaşmasıdır.

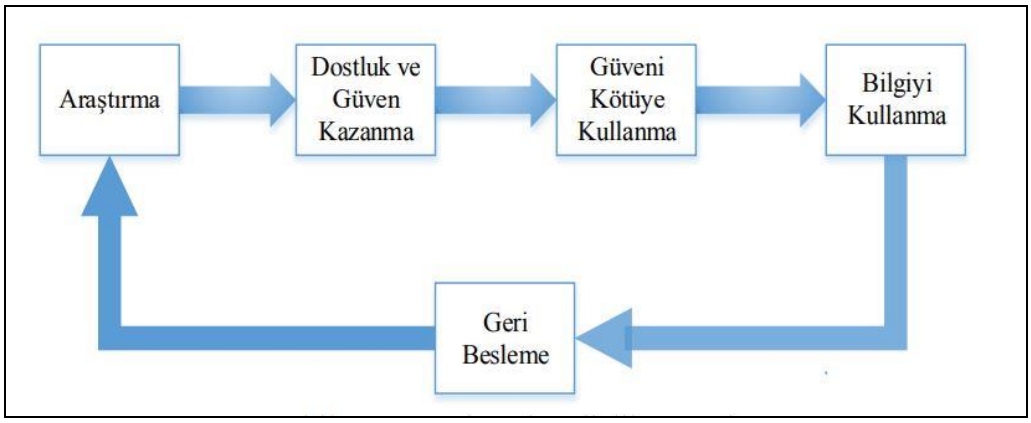
Teknik bilgi olmadan da gerçekleştirilebilen sosyal mühendislik saldırılarının ilk adımı, hedef sistem veya kullanıcı üzerinde veya ara kullanıcılar üzerinde araştırma ve keşif yapılmak ve ortaya çıkan zayıflıktan yararlanarak hedef psikolojisini veya kurum yapısını çözümleyerek saldırı planlamaktır. Saldırganlar sıklıkla kurum personeli, müşteri temsilcisi, yetkili personel kılıklarına bürünmektedir.

Gündüz & Daş, sosyal mühendisliğin uygulanmasındaki süreci;

> Sosyal mühendisin kurban hakkında araştırma yapması, kurbana karşı güvenini sağlamak amaçlı hareket, davranış ve eylemlerde bulunması ile istediği bilgiyi elde etmesi olarak görülür. Elde ettiği bu bilgiyi kullanacağı amaç doğrultusunda dener. Başarısız olması durumunda bilgi elde ettiği kurban, yani kaynağa tekrar bağlantı sağlayarak elde ettiği bu bilgileri sosyal mühendislik yöntemleri ile doğrulatabilir. Sosyal mühendislikte veri kaynağına tekrar ulaşabilmek için açık kapı mutlaka bırakılır. [24]

Şeklinde tanımlamış ve şekil de göstermişlerdir.

[24] Gündüz, M. Z., & Daş, R. (2016). Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri.



Şekil 2.4. Sosyal mühendislik süreci (Gündüz & Daş, 2016)

Teknolojinin kullanılmasından ziyade insan tabiatındaki birtakım zafiyetlerinden (güven duyma ihtiyacı, aceleci davranma, korku, merak vb.) faydalanarak, insanları etkileme ve ikna etme yöntemlerini kullanarak veya hile ile kandırarak, kurbandan bilgi alma ya da istenen işleri yapmasını sağlamak olarak tanımlanmaktadır. (Tombul, Güneştaş, & Başıbüyük, 2015)

Sosyal mühendislik saldırıları karşı tarafın zafiyetlerinden yaralanarak zekâ ürünü olarak kurgulanmış saldırılardır. Belirli bir sınırlaması olmamakla birlikte popüler sosyal mühendislik saldırıları şunlardır. (Rouse, 2018) ;

- Yemleme (Baiting): Saldırganın içerisinde zararlı yazılım olan donanımları bulunacağından emin olduğu bir ortamda bıraktığı ve kurbanın açgözlülüğü veya merakını yüzünden söz konusu harici bellek vb. dijital ortamdaki ürünleri kullanması ile gerçekleşen yöntemdir.
- Kimlik Avı Dolandırıcılığı (Phishing): Genellikle güvenilir bir kaynaktan geldiği imajı yaratan ve kurbanlarda aciliyet, merak veya korku duygusu yaratmayı amaçlayan e-posta ve kısa mesaj göndermek suretiyle, hassas bilgileri çalma, kötü amaçlı web sitelerine linkleri tıklatma veya kötü amaçlı yazılım içeren ekleri açmalarını sağlayarak gerçekleşen yöntemdir.
- Mızrak Kimlik Avı (Spear phishing): Mızrak avı, normal kimlik avı dolandırıcılığından farklı olarak saldırganın belirli kişileri veya işletmeleri seçtiği kimlik avı dolandırıcılığının daha hedeflenmiş bir sürümüdür.

- ❖ Telefon Dolandırıcılığı (Voice Phishing): Kimlik avı dolandırıcılığı yönteminin telefon kullanılarak yapıldığı yöntemdir. Ülkemizde telefon dolandırıcılığı olarak bilinen bu yöntem banka kanalları üzerinden sıkça kullanılmaktadır.
- ❖ Sahte Senaryolar Uydurma (Pretexting): Bir kişiden kişisel ve hassas bilgiler elde etmek amacıyla senaryolar üreterek kurgusal bir durumun yaratıldığı saldırı yöntemidir. Hedefin belirlenmesi, hedefe dair bilgi toplanması ve sahte bir senaryo/hikaye uydurarak manipülasyon ile istenilen bilgilerin elde edildiği sosyal mühendislik türüdür.
- ❖ Sahte Antivirüs (Scareware): Hedefin bilgisayarına kötü amaçlı yazılım bulaştığını veya yanlışlıkla yasadışı içerik yüklediğini düşünmesini sağlayan senaryolarla korkutma ve kandırma ve mağdura sahte sorunu çözecek asıl zararlı yazılımı almaya teşvik ederek yapılan saldırı türüdür. Yaygın örneği ise, internette gezinirken tarayıcınızda açılan pop-up pencerelerinde yer alan "Bilgisayarınıza virüs bulaşmış olabilir, virüs tespit edildi." vb. yönlendirici mesajlardır.
- ❖ Saptırma hırsızlığı: Bu tür saldırıda, bir teslimatı veya ödemeyi yapanı ya da kurye şirketini aldatarak, adres veya ödeme değişikliğine ikna ederek teslim edilecek ürünü veya ödemeyi ele geçirme şeklinde gerçekleştirilen saldırılardır.
- ❖ Quid pro quo: Bir şey için bir şey, anlamına gelen bu yöntem; saldırgan bilgisi veya yardımı karşılığında fayda sağlamayı iddia ederek ve hedeften kritik bilgileri ele geçirmeye çalıştığı, sıklıkla BT personeli rolüne bürünen saldırganların hedeflerine gerekli adımlar konusunda rehberlik ederek; kurbanların bilgisayarlarına veya kötü amaçlı yazılım başlatma yeteneğine erişmesini sağlaması şeklinde gerçekleşir.
- ❖ Yanına Takılma (Tailgating): Piggyback(omuzunda) olarak da bilinen yöntemde saldırgan yetkili bir giriş kartına sahip birini takip ederek erişim yetkisi olmayan güvenli binaya girerek hedef sisteme fiziksel erişim imkânı kazandığı saldırı yöntemidir.
- ❖ Omuz Sörfü: Hedefin kişisel erişim bilgilerini elde etmek için şifre yazılırken ya da erişim kısıtlı sistemlere girilirken fiziki yakınlıkla-omuzu üstünden bakarak- dürbün ve kamera sayesinde belirli bir mesafeden de yapılabilen saldırı yöntemidir. Kişilerin konuşmalarına kulak kabartarak elde edilebilecek bilgilerden de yararlanılabilmektedir.

Siber güvenlik alanın gelişmesi ve saldırı silahlarına karşı savuma sistemlerinin güncelliğini her an koruması bilişim sistemlerine saldırılarda en zayıf halkayı insan unsuru yapmıştır. Teknik olarak alınacak bütün tedbirleri baypas ederek saldırı için en uygun ortam ve imkânı

sunan sosyal mühendislik saldırılarının engellenmesinin en etkin yöntemi insan unsurunun eğitim ile bilinçlendirilerek güçlendirilmesidir.

Devlet veya özel bir kurumda veya şirkette gizli bilgilere erişim yetkisi olan veya ticari sırlara hakim bir personelin zafiyet göstermesi geri dönüşü imkansız sorunlara yol açabilecektir. Teknolojik olarak engellenmesi imkansız olan bu saldırı türünün en etkin mücadele yöntemi sürekli bilinçlendirme faaliyeti olacaktır.[25]

2.3.2.2. DNS - İP aldatmacası - ağ dinleme (Network sniffing) saldırı süreçleri

Kullanıcıların dikkatsiz kullanımı sonucu saldırganların şahısların bilgisayar ağları üzerinde değişiklik yaparak genellikle yönlendirme işlemi sonrası trafiğindeki paketlere-verilere erişim elde etmesidir. Kurumsal ağlarda ve bireysel kullanımlarda ağa erişim yetkisi elde ederek ağda dns-ip-mac aldatmacası yapılması gerektiği için teknik kapasitesi yüksek saldırganlar tarafından kullanılan bir yöntemdir.[26]

İP aldatmacası, sahte bir İnternet Protokolü (IP) adresi üzerinden bağlantıyı ele geçirmeyi ifade eder ve bilgisayarın IP adresini maskeleme eylemidir. Bir web sayfası ziyaretçisi girmek istediği adres yerine korsan tarafından oluşturulan web sayfasına yönlendirilmekte ve ziyaretçi bu sayfa ile dinamik bir etkileşime geçtiğinde ise siber korsan önemli bilgilere, bilgisayar veya ağ kaynaklarına erişebilir hale gelmektedir. (Türkay, 2013)

İP aldatmacası, özellikle hizmet dışı bırakma saldırılarında (DOS, DDOS) sıkça kullanılmakta ve ayrıca hedef bilgisayarı aldatmak için İP adresine dayalı kimlik doğrulama sistemlerinde de kullanılabilmektedir. İP aldatmacasında hedef bilgisayarlara yetkisiz erişime izin vermesi değil, DDOS saldırıları için bilgisayar oturumlarını ele geçirmektir.

Alan adı sistemi (DNS) aldatmacası (DNS önbellek zehirlenmesi), değiştirilmiş DNS kayıtlarının çevrimiçi trafiğini, hedeflenen yere benzeyen sahte bir web sitesine yönlendirmek için kullanıldığı bir saldırıdır. Alan adı sunucusunun önbellek veritabanına eklenen verilerle yada oradaki verilerin sabote edilmesi ile hedef bilgisayarın saldırganın belirlediği ip adresine yönlenmesi sağlanmaktadır. Kullanıcıların gerçek siteye giriş için kullandığı bilgiler bu sayede eke geçirilmiş olur ve hedef bilgisayara zararlı yazılım yüklemesi de çok olası bir durumdur.

[25] Fan, W., Kevin, L., & Rong, R. (2017). Social engineering: Ie based model of human weakness for attack and defense investigations. *IJ Computer Network and Information Security*, *9*(1), 1-11.
[26] GÜNDÜZ, M. Z. (2013). Bilişim suçlarına yönelik IP tabanlı delil tespiti/IP-based evidence detection.

DNS aldatmacası (zehirlenmesi) gerçekleştirme yöntemleri[27] [28]şunlardır:

- ❖ Ortadaki adam (MITM) - Kullanıcıları farklı / kötü niyetli bir IP adresine yönlendirmek için kullanıcılar ve bir DNS sunucusu arasındaki iletişimin kesilmesi.
- ❖ Sunucu Ele geçirilmesi - Kötü niyetli bir IP adresi döndürmek üzere yapılandırılmış bir DNS sunucusunun doğrudan ele geçirilmesi.
- ❖ DNS önbellek zehirlenmesi - Sunucusunun ön bellek veritabanına veri eklenerek, ya da oradaki veriler değiştirilerek ad sunucunun yanlış IP adresleri dönmesine ve trafiğin başka bir bilgisayara genelde de saldırıyı yapanın bilgisayarına yönlendirilmesine neden olan bir saldırıdır.

Buradan da anlaşıldığı üzere bazen gerçek olduğunu zannederek girdiğimiz bir site aslında saldırganlar tarafından oluşturulmuş gerçeğine benzer sahte bir site olabilir. Bu durumda kişisel giriş bilgilerimizi şifrelerimizi girmemiz bu bilgileri karşı tarafa teslim etmiş olacağımızdan girmiş olduğumuz sitenin mahiyeti boyutunda bireysel kullanımlar için ekonomik, bir kuruma yönelik durumlarda ise gizli bilgilerin ele geçirilmesi boyutunda olabilmektedir.

Saldırganların saldırı unsurlarını devreye sokmak için sistem üzerinde zayıf noktaları gözlemlediklerine değinmekte de yarar var. İletişim ağından dolaşan şifrelenmiş veya şifresiz verilerin saldırganlar tarafından sistem zafiyeti tespit etmek veya saldırmak için teknik yöntemlerle dinlenmesi ele geçirilmesi ise ağ dinleme olarak isimlendirilmektedir.

Kullanıcılar arasındaki bilgi alışverişi ortamının dinlenmesine "monitoring" yani aktif dinleme, bilgi alışverişini kullanılan bilgilerin içeriklerinin yakalanmasına "sniffing" pasif dinleme veya "koklama" denir. (Çifçi, 2013) (Ulaşanoğlu, Yılmaz, & Tekin, 2010) Kullanıcılar günlük rutinlerinde işlemlerini yürütürken ağa ait bileşenler üzerinden verilerin transfer sürecine müdahale ile yapılan bir yöntem olması sebebiyle sistemsel verilerin akışının da kontrol edilmesi ile tespit edilebileceği için yazılımsal, fiziksel güvenlik dışında ağ güvenliğinin alınması da bu sebeple çok önemli konuma gelmiştir.

Ulaşanoğlu ağ tarama süreci unsurlarını,[29]

[27]https://medium.com/@oguzalbastr02/ortadaki-adam-sald%C4%B1r%C4%B1s%C4%B1-mitm-detayl%C4%B1-anlat%C4%B1m-5e5f86af1d6a Erişim Tarihi: 20.07.2019

[28] ŞEN Ş. & AKGÜN F. & BULUŞ E. Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler Ve Korunma Yollarının İncelenmesi.

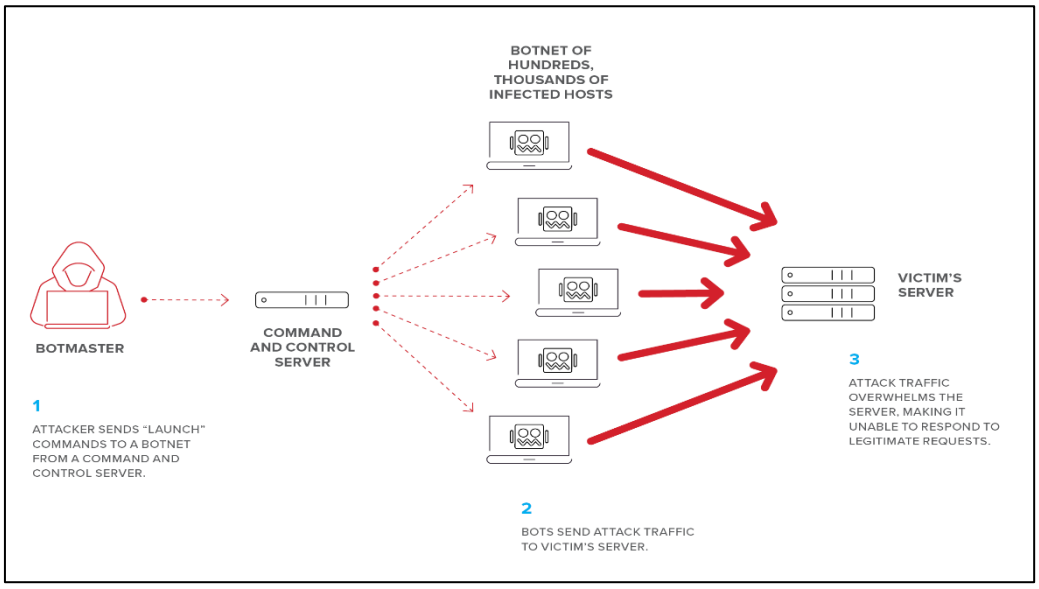
[29] Ulaşanoğlu, M. E., Yılmaz, R., & Tekin, M. A. (2010). Bilgi güvenliği: Riskler ve öneriler. *Bilgi Teknolojileri*.

"…şebeke ortamındaki bilgisayarlar arası veri paketlerinin izinsiz ve yetkisiz bir şekilde dinlenmesidir. İnternet paketleri gönderilen lokasyona yönlendirici (router) denilen şebeke elemanlarından, çoklayıcılardan (hub), anahtarlama elemanlarından (switch) ve şebeke kablolarından ya da havadan telsiz haberleşme dalgalarından geçerek ulaşmaktadır. İnternetteki veri paketleri iki kısımdan oluşmaktadır. İlk bölümde gidecekleri yerin IP adresi, ikinci bölümde de içerdikleri bilgi bulunur. Yönlendiriciler kendilerine gelen paketi ilk bölümde yazan IP Numarasına ait adrese en yakın yönlendiriciye gönderir. Yerel şebekelerde ise makineleri birbirine bağlarken çoklayıcılar kullanılmaktadır."

şeklinde ele almış ve özetlemiştir. Sistem içine girebilmek için açık pencere arama yöntemidir ağ dinleme. Ağda açılacak veya güvenliği alınmamış bu noktalar veri bütünlüğünün sağlanamamasına sebep olarak sistemde ciddi zafiyetlere sebep olabilmektedir.

2.3.2.3. DOS – DDOS saldırıları çalışma sistemi (Hizmet reddi saldırısı)

Diğer saldırı örneklerini aksine hizmet aksatma saldırıları sisteme giriş veya sistemde açık yaratma, sisteme zararlı yazılım yükleme, veri veya bilgi elde etme şeklinde gerçekleşmemektedir. Yukarıda örneklerini vermiş olduğumuz siber silahlar ile ele geçirilmiş kullanıcı hesapları kullanarak farklı bir sistemi hedef alan saldırılardır. DOS (Denital Of Service) ve Ddos (Distributed Denital Of Service) saldırıları, normal şartlar altında istemcilere hizmet edip cevap vermesi gereken sunucuların bir şekilde cevap veremez duruma getiren saldırı tipidir.



Şekil 2.5. DDOS saldırı şeması

Dos saldırısı yapılan sunucu hizmet bekleyen kullanıcılara hiç hizmet vermeyebilir veya çok yavaş bir şekilde hizmet vermeye devam eder.[30] Adından da anlaşılacağı gibi, hizmet reddi saldırısı, saldırganların kullanıcıları ağa bağlı bir sisteme, hizmete, web sitesine, uygulamaya veya başka bir kaynağa erişmelerini engelleme girişimidir. Saldırı tipik olarak bir sistemin yanıt vermesini yavaşlatır veya sistemi tamamen devre dışı bırakabilir.[31]

Dos saldırısı tek bir kaynaktan hedefe doğru yapılmaktadır. Şekil 2.5'te gösterildiği şekilde Ddos saldırısında ise birçok kaynaktan yapılmakta ve şiddeti daha fazla olmaktadır. Bir Dos saldırısı yapmak için saldırganın ileri seviye bir uzman olması gerekmemekte ve fazla bir teknik bilgiye ihtiyacı olmamaktadır. Önemli olan saldırganın elinde bulunan istemci gücüdür. Elinde ne kadar çok istemci bulunuyorsa, sunucudan anlık olarak isteyeceği cevap sayısı o kadar yüksek olur. Bir süre sonra bu istekler sunucunun cevap veremeyeceği kadar yüksek olacağından sunucu isteklere cevap veremez hale gelir ve Dos saldırısı gerçekleşmiş olur. [32] Dos saldırılarının başarılı olmasını sağlayan ana etken, her sunucunun belirli bir kapasiteye sahip olmasıdır. Ddos saldırısının etkilerini artırmak amacıyla saldırganlar botnetler de kullanabilmektedir.[33]

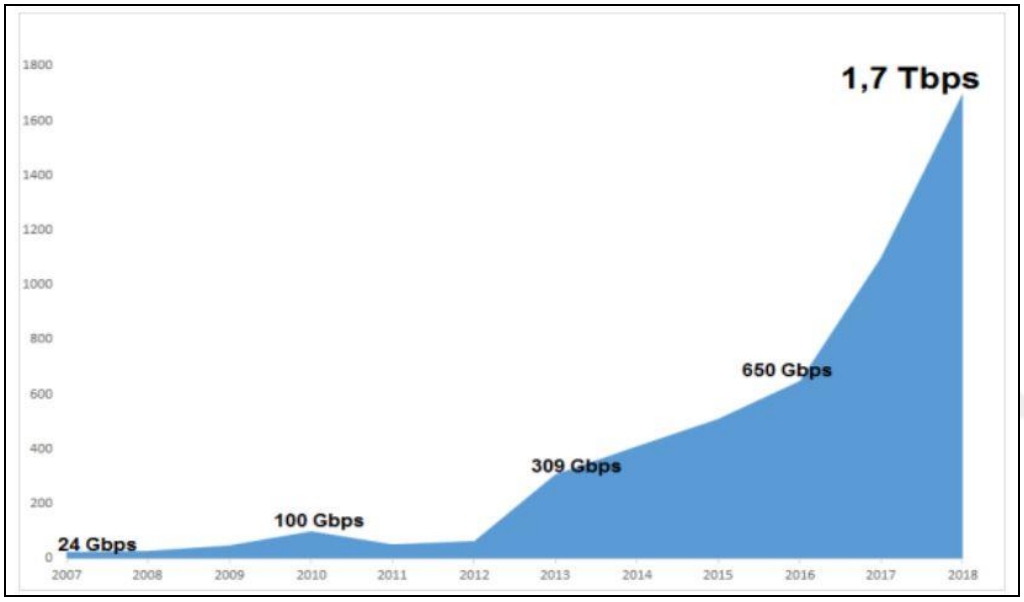
Kelimenin tam anlamıyla onlarca farklı DDoS saldırısı türü olduğu için, bunları basit veya kesin olarak sınıflandırmak zordur. Bilinen en yaygın üç kategori hacimsel, protokol ve uygulama katmanıdır, ancak bunların hepsinde örtüşme vardır. Örneğin, bazı protokol saldırıları hacimsel de olabilir.

Sel olarak da bilinen hacimsel saldırılar, en yaygın DDoS saldırısı türüdür. Genellikle kullanıcıların erişiminin reddedildiği kadar fazla bant genişliği kullanmak amacıyla hedeflenen mağdurun ağına büyük miktarda trafik gönderilerek gerçekleştirilir. Saldırganlar genellikle hedef ağa veya sunucuya ulaşan trafik hacmini artırmak için botnet'leri kullanırlar. Botnet kullanımı, hedef sistemin kendi ağlarında gerçekleştirebileceği kapasitenin yani bant genişliğinin ötesinde, saniyede yüzlerce gigabayttan terabitlere kadar değişen devasa DDoS saldırıları yapılmasına olanak sağlamıştır.

[30] Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643-666.
[31] ATASEVER, S., ÖZÇELİK, İ., & SAĞIROĞLU, Ş. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *23*(1), 238-244.
[32] https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack- Erişim Tarihi 12/11/2019
[33] Özocak, G. (2012). DDoS Saldırısı ve Failin Cezai Sorumluluğu. *Bilişim*, *28*, 23.

Symantec 2017 İnternet güvenliği risk raporuna göre[34]; bir web sitesine yönelik yapılan saldırı o yıla kadar raporlanan en büyük DDoS saldırısı olmuş ve 620 Gbps seviyesine ulaşmıştır. Yine 2017 yılında Fransız servis sağlayıcı OVM, 1Tbps seviyesinde DDoS saldırısına maruz kaldığını açıklamıştır. Aynı içerisinde boyutun bu denli büyümesi botnet sayısının giderek artışının da bir göstergesi olmuştur.

Arbornet 2018 kayıtlarına[35] göre hazırlanan DDoS saldırılarının maksimum bant genişliği sayıları Grafik 2.6 da gösterilmiştir. Botnetler sayesinde ulaşılan bant genişliği boyutu internette yayın yapan bütün küçük çaplı sitelerin tehdit altında olduğunun göstergelerinden biridir.



Grafik 2.6. Ddos bant genişliği boyutları Kaynak: Arbornet

Protokol saldırıları ise sunucuları hedeflemek yerine, protokollerin zayıf yönlerini veya normal protokol davranışlarını kullanarak hizmeti reddi gerçekleştirir. Amaç, ağın veya ara kaynakların (güvenlik duvarları gibi) hesaplama yeteneklerini tüketerek hizmet reddine neden olmaktır. Protokol saldırıları paket düzeyinde gerçekleştiğinden, genellikle saniye başına paket cinsinden ölçülürler.

Uygulama katmanı saldırıları ağ sunucularının yerine web sunucularını, web uygulama platformlarını ve belirli web tabanlı uygulamaları hedefler. Saldırganın amacı, sunucuyu çökertmek, bir web sitesini veya uygulamayı kullanıcılara erişilemez kılmaktır. Bu saldırılar

[34] Internet Security Threat Report. 2017. Symantec, 22.
[35] Arbour Networks, 2017. "Current DDoS attacks", http://www.asiapacificsecuritymagazine.com/w p-content/uploads/2017/01/2017-01-19- Arbor-WISR-Full-Report.pdf

bilinen uygulama açıklarını, uygulamanın altında yatan iş mantığını hedefleyebilir veya HTTP / HTTPS ve SNMP (Basit Ağ Yönetimi Protokolü) gibi daha yüksek katman protokollerini kötüye kullanabilir. Bu saldırılar genellikle diğer saldırı türlerine göre daha az bant genişliği kullanır ve bu nedenle trafikte her zaman ani bir artış göstermez ve bu da tespit edilmelerini zorlaştırır. Uygulama katmanı saldırıları saniyede yapılan isteklerde ölçülür.

Bu ve benzer şekilde sisteme doğrudan zarar verme çabası olmadan dolaylı yol ve yöntemlerle yapılan saldırıların motivasyonu farklılık göstermekle birlikte büyük çoğunluğu[36] sosyal ve politik açıklama yapmak isteyen hacktivist gruplar, bir şirketin, grubun ve kimi zaman devletin gelirini ve imajını olumsuz yönde etkilemek isteyenler, bireysel olarak fidye yöntemi ile para temin etmeye çalışanlar şeklinde dağılım göstermektedir.

İlerleyen bölümlerde detaylı örneğini vereceğimiz Stuxnet olayı ve yakın zamanda ülkemizde meydan gelen ddos saldırısı[37] direkt olarak kuruma ait sisteme zarar vermeye çalışmamakla birlikte yüzbinlerce kişiye hizmet veren kurumların hizmet aksaması dolaylı dahi olsa ciddi boyutlara ulaşabilmektedir. Bu tarz büyük saldırı planları yapılabildiği gibi bireysel hedeflere yönelikte saldırı planları yapılabilmektedir.

2.3.2.4. Phishing (Oltalama) saldırı şekilleri ve istatistikleri

Siber uzayın bilinen en meşhur saldırı yöntemi olan oltalama saldırısı dolandırıcılığın bilişim sistemi üzerinde tezahürüdür ve içeriğinde çoğu zaman sosyal mühendislik unsurları barındırabilmektedir. Hedef kullanıcıdan genellikle bankacılık işlemlerine ait kişisel bilgilerin temin edilmesi için oluşturulan sahte bir site veya içeriğinde zararlı yazılım içeren mail veya mail trafiğine müdahale şeklinde gerçekleşmektedir.[38]

Phishing saldırılarında temel amaç, kullanıcıyı belli bir eylemi yapmaya (genellikle bir bağlantıyı tıklamaya veya bir uygulamayı çalıştırmaya) ikna ederek kişisel bilgilerini çalmak ve bu bilgileri kötü amaçla kullanmaktır. Farklı yöntemlerle phishing saldırıları düzenlenebilir.

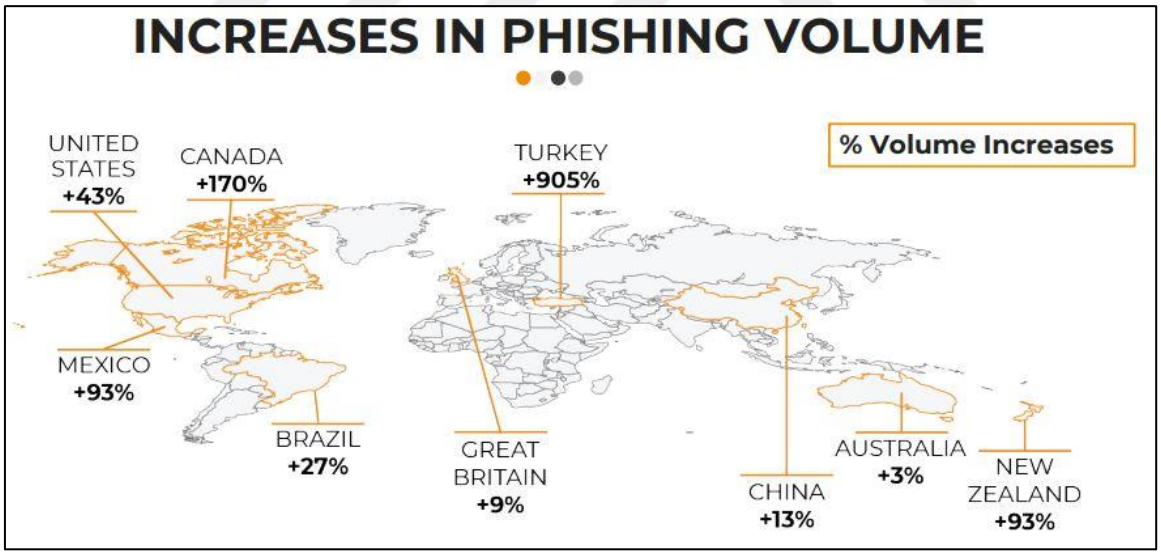
Phishing (Oltalama) saldırısı güvenilir bir elektronik haberleşme aracı gibi görünerek kullanıcı adı, şifre, kredi kartı bilgileri vb. özel bilgilerin kötü amaçla ele geçirilmesidir. İlk

[36] https://www.trustedknight.com/ddos-attacks-3-common-motivations/ Erişim tarihi: 15/11/2019
[37] http://www.hurriyet.com.tr/teknoloji/turkiyeye-siber-saldiri-soku-turk-telekomdan-flas-aciklama-geldi-41360791
[38] HEKİM, H. Oltalama (Phıshıng) Saldırıları.

olarak sahte bir e-posta veya farklı bir elektronik ortamdan mesaj ile kullanıcıyı gerçeğine çok benzeyen sahte bir web sitesine yönlendirerek, kullanıcının kişisel bilgilerini buraya girmesi sağlanır. Çevrimiçi bir saldırı türüdür. Bu saldırıda en zayıf halka insan faktörüdür. Phishing yönteminin en sık kullanılan üç çeşit saldırı tipi vardır.[39] Bunlar Spear (Mızrak) Phishing, Clone(Klon) Phishing ve Whaling (Balina Avı) tipi saldırılardır.

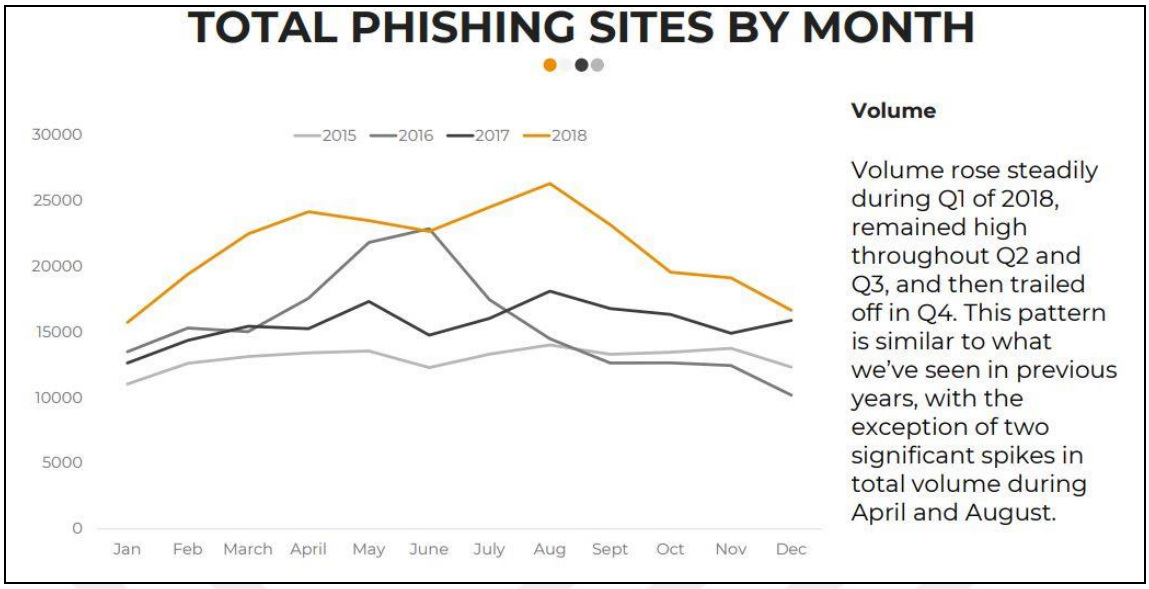
Spear Phishing saldırısında saldırgan hedefe yönelik istihbarat toplar ve bu bilgileri kullanarak hedefi bir linke yönlendirmeyi amaçlar. *Clone Phishing* saldırısında saldırgan Gmail, Facebook gibi ünlü uygulamaların benzerini üreterek buradan kurbanın kullanıcı adı ve şifre bilgilerini ele geçirmeyi amaçlar. *Whaling* bir şirketten hassas bilgileri çalmak için CEO gibi yüksek profilli çalışanları hedef alan saldırı türüdür.

Saldırıların büyüklüğü sebebiyle bu ismi almaktadırlar. Bu saldırılarda da sosyal mühendislik önemli bir yer tutar. En bilinen saldırı olmasının sebepleri başında, siber güvenlik kuruluşu Pishlabs[40] tarafından hazırlanan *"*2019 PHISHING TRENDS AND INTELLIGENCE REPORT The Growing Social Engineering Threat*"* raporunda yer alan grafikte de görüldüğü üzere oltalama sitelerinin artışı gelmektedir.



Şekil 2.6. Ülkelerin phishing (Oltalama) artış durumu

[39] https://www.binance.vision/tr/security/what-is-phishing
[40] https://www.phishlabs.com/about/



Grafik 2.7. Oltalama sitelerinin aylık grafiği

Oltalama sitelerinde sosyal mühendislik unsurlarının yer aldığını Grafik 2.8 de yer alan önemli gün ve haftalardaki artış sayılarından[41] da anlayabilmekteyiz. Bu günlerde kişilerin dalgınlık, yoğunluk zafiyet veya temin etmesi gereken ürün vb ihtiyaçları üzerinden kurgulama yaparak oltalama saldırılarında artış meydana getirmektedirler. Ülkemizin ise oltalama türü saldırıların en çok artı gösteren ülke konumunda olduğunu Phislabs raporundan okuyabiliyoruz.

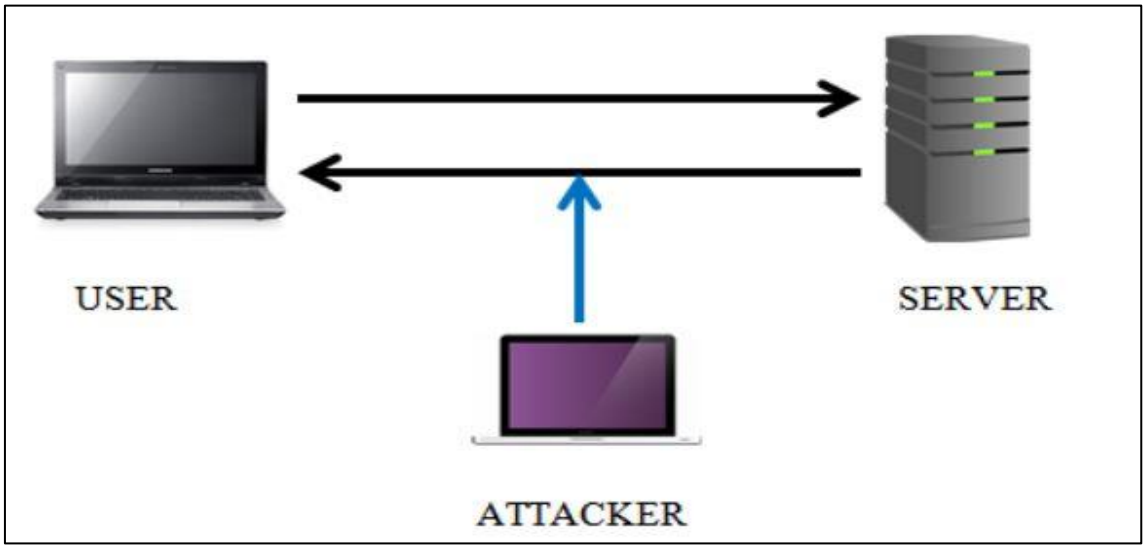
Grafik 2.8. Phishing önemli gün ve haftalardaki artış oranları

[41] https://www.f5.com/labs/articles/threat-intelligence/2019-phishing-and-fraud-report

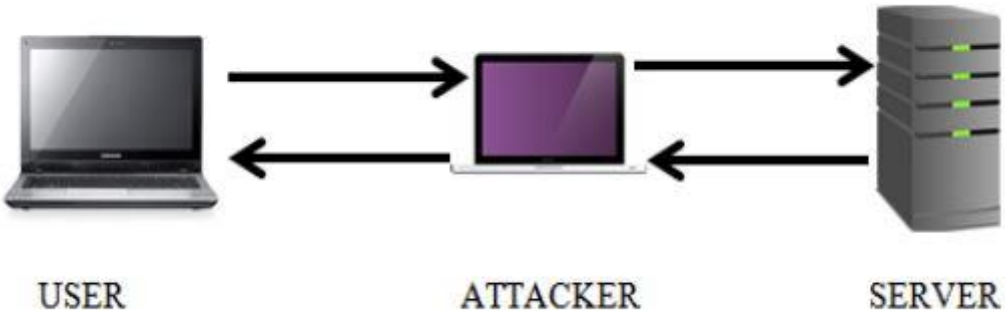
İnternet kullanımının hızla arttığı ve artık nesnelerin interneti boyutuna geçtiğimiz bu çağda suçluların da teknolojik gelişim geçirdiğini göz ardı etmeden bireysel güvenliğimizi alarak hareket etmeliyiz. Devletler için ise kayıplar sadece maddi olmanın ötesinde güvenlik alanında olabilmektedir. Oltalama saldırısına maruz kalan bir yetkili oturum çalma saldırısına da kapı aralamış olacaktır.

2.3.2.5. Oturum çalma – yerine geçme (Session hijacking) ve arka kapı (Backdoor-trapdoor)

Siber saldırı, kişi veya kurumların farklı cihazlar üzerinden kullandıkları oturum hesaplarını ele geçirerek verilere ulaşmak şeklinde de karşımıza çıkabilmektedir. "Session hijacking" kelime anlamı olarak "oturum çalmak" demektir. İki aygıt arasındaki TCP iletimini ele geçirmeyi amaçlayan bir saldırı türüdür. Doğrulama işlemi TCP oturumu başlangıcında olduğundan bu, saldırganın makineye erişimine olanak sağlar. Bu işlemde saldırgan geçerli oturum ID' sini çalarak sunucuya kendisini doğrulatır. Oturum ele geçirme aktif saldırı ve pasif saldırı olarak ikiye ayrılır. Aktif saldırı, saldırganın kullanıcı ve sunucu arasında zaten etkin olan oturumda saldırdığı bir tekniktir.(Grafik 2.4) Pasif saldırı da ise kendisini geçerli kullanıcı ve sunucu arasına sokarak kullanıcıya bir sunucu olarak ve sunucuya geçerli bir kullanıcı olarak maskelenerek kullanılan tekniktir.(Grafik 2.5) (Baitha & Vinod, (2018)



Grafik 2.9. Aktif oturum çalma, Kaynak: (Baitha & Vinod, (2018)



Grafik 2.10. Pasif oturum çalma, Kaynak: (Baitha & Vinod, (2018)

İnternet ağı üzerinden faaliyet gösteren bir devlet kurumunda yetkili bir personelin oturumun saldırganlarca ele geçirilmesi en temelde veri hırsızlığa sebep olabileceği gibi veri üzerinde değişiklik yapılarak ekonomik kazanç da elde edilebilir. Teknik olarak yapılabilir görülen bu saldırı ülkemizde güvenlik güçlerimizin yerel ağ kullanması[42] sebebiyle güvenlik unsurları boyutunda zor bir saldırı türüdür. Ağ üzerinde oluşacak bir açıkta ise farklı bir saldırı türü olan Arka kapı saldırısı (Backdoor) ortaya çıkacaktır.

Arka kapı (Backdoor) saldırıları bir sisteme uzaktan erişim sağlayabilmek amacıyla, sistemde bulunan açıklardan yararlanarak normal kimlik doğrulama prosedürlerini ihmal eden saldırı yöntemidir. Bir sisteme sızmada kullanılan saldırı yöntemleri arasında oldukça popüler bir yöntemdir. Arka kapılar sistem geliştiricisi tarafından test amacı ile sisteme erişmek için kullanılan ve daha sonra bu şekilde unutulan açıklardan veya saldırganlar tarafından yazılmış kod parçalarının bilgisayara yüklenmesi ile oluşmaktadır. Bu şekilde arka kapıları kullanarak saldırı yapan kötü niyetli kişiler, sistem üzerinde program çalıştırma, kişisel dosyalara erişme, dosyalarda değişiklik yapma, dosya yükleme, kullanıcının klavye hareketlerini izleme ve spam e-posta gönderme vb. gibi birçok eylem gerçekleştirebilirler.

Devletlerin bilişim güvenliğine yönelik yapılan saldırılarda sistem yöneticilerince tesis edilen eksik bir güvenlik prosedürü sonucu ortaya çıkabilecek bu saldırı türünde kayıp verilerin karşı tarafın eline geçmesi şeklinde olacaktır.

2.3.2.6. SQL enjeksiyonu ve diğer saldırı yöntemleri

Bilgisayarın temel çalışma unsurları olan programlar veya internet ağının unsuru olan web siteleri çeşitli yazılım dilleri ile inşa edilmektedir. Yazılımsal boyutta da olabilecek açıkları

[42] https://www.egm.gov.tr/bilgiteknolojileri/projeler Erişim Tarihi: 16/11/2019

arayan saldırganların başvurduğu bu yöntem yazılım dili üzerinde siteye vere programa girme oturum ele geçirme veri alma şekillerinde olabilmektedir.

Siber ortamda bulunan verilere ulaşmak için kullanılan web sayfaları aynı zamanda saldırganlar içinde veri tabanlarına ulaşmak için kullanılan en kullanışlı aracıdır. Genellikle bu tür saldırılar, uygulama katmanı üzerinden gerçekleşmektedir. Diğer bir ifade ile web uygulamalarına saldırılar düzenleyerek, veri tabanına ulaşmak ve hatta site üzerindeki verilerde manipülasyon yapmak mümkündür.

Bu şekilde yapılan saldırılara ismini veren *SQL* (Structured Query Language*)* veri tabanlarından data çekme, değiştirme ve silme gibi işlemler için kullanılan basit yapılı bir programlama dilidir.[43] SQL injection, web sayfalarının ara yüzünü kullanarak veri tabanlarına erişmek için SQL sorgusu ve komutu gönderme tekniğidir. Web sitesi ara yüzü ile eklenen SQL komutları SQL sorgusunu değiştirebilir ve web uygulamasının güvenliğini tehlikeye sokabilir. Yani SQL injection yöntemi ile saldırgan yönetici şifreleri, üye bilgileri gibi veri tabanlarını bulup, herkese açık olmayan bu bilgilerden yararlanabilir.

En basit SQL injection kullanıcı girişi sırasında yapılan saldırıdır. Web uygulamasına olası üye girişi işlemi şu şekilde gerçekleşir, web sayfası ara yüzünde oluşturulan formdan gelen kullanıcı adı ve şifre bilgisi ile ilgili SQL cümleciğini oluşturulur*(select * from members where user='admin' and password='sifre'),* SQL sorgusu kayıt döndürüyorsa böyle bir kullanıcının var olduğu anlamına gelir ve oturum açılır ve ilgili kullanıcı üye girişi yapmış olur. Eğer veri tabanından kayıt dönmediyse "*kullanıcı bulunamadı*" veya "*şifre yanlış*" gibi bir hata ile tekrar üye girişi formuna geri dönülür.

Günümüz büyüyen teknolojik ağlarında üye olduğumuz birçok adres büyük tehlikelere kapı aralayabilir. Bireyin kendi güvenliğini temin etmesi dışında kullanmış olduğu web sayfaları da tedbirli olmalı ve güvenliği almış olmalıdır.

Cross-Site Scripting (XSS) Siteler Arası Betik Çalıştırma açığı, web sayfalarınızda meydana gelen veri giriş alanlarındaki açıklarından faydalanılarak bu alanlarda HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla tarayıcı üzerinden javascript kodlarının çalıştırılabilmesi yöntemidir. Uygulama programlayanların "meta karakter filtrelemesi" yapmamalarından ve son kullanıcıdan alınan değerlerin, gerekli HTML ve JavaScript filtrelerinden geçmemesi sebebiyle kullanılan bir yöntemdir. XSS açığı, Reflected XSS,

[43] https://veriakademi.com/sql-nedir

Dom-Based XSS ve Stored XSS olmak üzere üç türe ayrılmaktadır. (Çıtak, 2016) Cross-site Request Forgery (CSRF) Siteler Arası İstek Sahtekârlığı açığı; web uygulama kullanıcısının, uygulamaya gönderilen isteklerin hangi kaynaktan geldiğinin kontrol edilmediği sistemlerde, işlem yapmaya yetkisi olmayan saldırganın kodlama açıklarından faydalanarak kullanıcıya ve uygulama üzerinden istem dışı işlemler yürütmesi ile ortaya çıkan bir saldırı türüdür.

İnternet ağının dünyanın her yerini sarmış olmasının bir sonucu olarak hızlanan iletişim ağı beraberinde çeşitli yenilikler getirmiştir. Bunlardan biri de kripto paralardır. Her siber uzay elemanında olduğu gibi kripto para sisteminde de siber saldırıların hedefi olmuş ve yeni saldırı türü olan yüzde 51 saldırısı[44] veya çoğunluk saldırısı ortaya çıkmıştır. Blok zinciri (blockchain) sisteminde gerçekleşen saldırı türüdür. %51 saldırısı, kötü niyetli saldırgan veya kuruluşun, blok ağın toplam gücünün yarısından fazlasını kontrol ederek, blok zincir sisteminin bütünlüğüne yönelik olarak ağı tehdit edebileceği, blok ağın birlik mekanizmasını geçersiz kılabileceği ve çift harcama gibi kötü niyetli davranışlarda bulunabileceği saldırı türüdür.

Blok zincirine yapılan %51 saldırı, mevcut bilinen ağların büyüklüğü nedeniyle pek mümkün gözükmemekte ve ağ büyüdükçe, diğer tüm katılımcıları bastırmak için yeterli ağ gücünü elde edebilecek kişi veya kuruluşun olma olasılığı daha da olanaksız hale gelmektedir. Fakat bu saldırı küçük blok zinciri ağları için hale tehdit olabilmektedir. Her yeni tekonojik gelişme insanların hayatına yenilik getirdiği gibi yeni suç türlerine de kapı aralamaktadır. Geçmişte yaşanan örneklere ileride oluşacak yeni saldırı türlerinin zararları konusunda bize ışık tutacaktır.

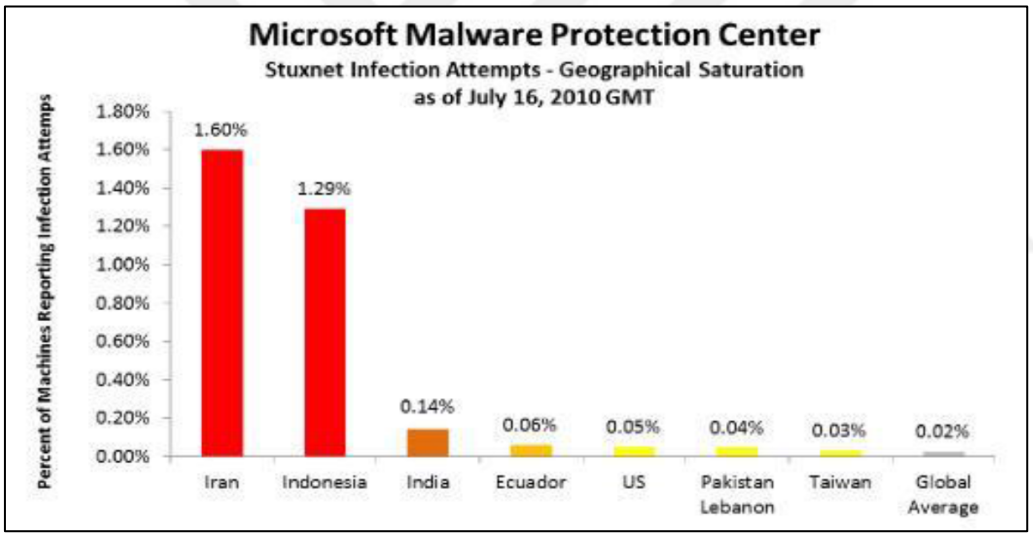
2.3.3. Siber Saldırı Örnekleri ve Güvenlik Alanına Etkileri

Siber uzayda karşımıza çıkan saldırı silahları ve siber saldırı türleri her an dünya üzerinde vuku bulmakla birlikte bazıları boyutu, tarafları veya sonuçları itibari ile bilinir hale gelmişlerdir. Çalışmamızda yer vereceğimiz örnekler sonuçları itibari ile güvenlik konusu alanına girdiği için tercih edilmiş ve süreç güvenlik alanına etkisi boyutunda kısa olarak örneklendirilmiştir.

[44] https://www.binance.vision/tr/security/what-is-a-51-percent-attack Erişim Tarihi: 13/11/2019

2.3.3.1. Stuxnet (2010) saldırısı ve siber güvenlik için önemi

Siber güvenlik tarihinin dönüm noktası olarak kabul gören Stuxnet saldırısı[45] 2010 yılında İran'a yapılmıştır. İran nükleer tesislerine sızma yoluyla bulaşarak, uranyum zenginleştirme programını yaklaşık 2 yıl sekteye uğratmıştır.[46] Stuxnet olayının en önemli özelliği, ağa bağlı olmayan sistemlere insan müdahalesi ile zararlı yazılımların yerleştirilip aktif hale getirilmesi sonucunda, siber saldırının gerçekleştirilmesidir. *Stuxnet* virüsü tüm dünyada yayılmasına rağmen en çok İran'ı hedef almıştır. Stuxnet virüsü, bir ana kartı hedef alacak şekilde programlanmış, kullanıcı bilgisayarlarına zarar vermemiştir. Bu sebeple yayılma tarzı, etkileri ve kullanış şekli bakımından diğer kötü amaçlı yazılımlardan çok farklıdır. İran nükleer tesislerinde çalışan birinin kasıtsız olarak veya Mossad için çalışan birinin kasıtlı olarak bilgisayara USB belleği takarak solucanı aktif hale getirdiği ve bu şekilde sistemde yayıldığı düşünülmektedir. (Aydın, 2013)



Grafik 2.11. Stuxnetin etkilediği ülkeler (Pamuk, 2012)

Zararlı yazılımların karşılaşılan en gelişmişi olan *Stuxnet*'in en önemli tarafı kendisini otomatik olarak kopyalayabilmesidir. Bulaştığı ağı etkisiz hale getirene kadar çoğalıp, yayılma özelliği göstermektedir. New York Times, BBC ve Guardian gibi gazeteler bu virüsün ABD veya İsrail tarafından geliştirildiğini düşünmektedir. Çünkü *Stuxnet*'in zarar verdiği sistemlerin %60'ı İran'da yer alan bilgisayarlardır. (Gürkaynak & İren, 2011)

[45] Hagerott, Mark (2014), "Stuxnet and the vital role of critical infrastructure operators and engineers", International Journal of Critical Insfrastructure Protection, 7, s.244

[46] Mueller Paul ve Yadegari Babak (2012), "The Stuxnet Worm", http://www.cs.arizona.edu /~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf (01.02.2016).s.10

Stuxnet virüsünden etkilenen bilgisayarların %60'ının İran'da bulunması bu virüsün İran nükleer sistemlerini hedef aldığı ve sadece bu maksatla yazıldığı yorumlarına sebep olmuştur. Petrol ve gaz hatları, elektrik üretim santralleri ve sanayi kuruluşlarında kontrol maksatlı olarak kullanılan sistem *Stuxnet* virüsü tarafından hedeflenen ana sistem olarak belirtilmiştir. (Ünver, 2011)

Stuxnet, sadece ağa bağlı bilgisayarların değil aynı zamanda dış dünyaya kapalı olan ICS'leri (Endüstriyel Kontrol Sistemleri) de hedef almış olması bakımından önemli bir yere sahip olup, siber saldırılara karşı farkındalık seviyesi gelişmemiş bu konuda hazırlığı bulunmayan ülkeler için bir uyarı niteliği taşımaktadır. (Çifçi, 2013)

Stuxnet bilgisayar virüsünün hedefi olan İran, uranyum zenginleştirme tesislerinin internet güvenliğini sıkılaştırmıştı. Tahran yönetimi daha önceki açıklamalarda Stuxnet'in ABD ve İsrail'in işi olduğunu öne sürmüş bağımsız internet güvenliği şirketlerinde bu açıklamaları teyit eden sonuçlara varmıştır.[47] İsrailli yetkililer batının İran'ın petrol ve bankacılık sektörüne uyguladığı yaptırımları Tahran'ın nükleer programını durdurmaya ikna etme konusunda başarısız olması durumunda ülkedeki nükleer tesislere askeri operasyon düzenleme tehdidinde bulunmuştur.

Bu örnek siber tehdidin her alanı hedef alabileceğini gösterdiği gibi ülke seviyesinde güvenlik açığı olabileceğine-oluşturabileceğine ve siber tehditlerin ülkeler düzeyinde casusluk aracı olarak kullanıldığı en bariz örnek olmuştur.

2.3.3.2. Shady RAT (2006 - 2011) saldırısı ve etki alanı

2006 ile 2011 yıllarında yapılmış olan APT (Advanced Persistent Threat) türündeki casusluk faaliyeti olan Shady RAT (Uzaktan Yönetim Aracı) saldırıları, McAfee'nin hazırladığı bir raporla 2011 yılında öğrenilmiştir. [48] Bu saldırılar sonucu birçok şirket, kurum ve kuruluş hedef alınmış ve böyle bir eylemin dünya piyasası üzerinde son derece etkili olduğu söylenebilir. Shady RAT etki ve süre bakımından bakıldığında, şimdiye kadar yapılmış en geniş çaplı siber saldırı türü olduğu değerlendiriliyor.[49] [50] (Çifçi, 2013).

---

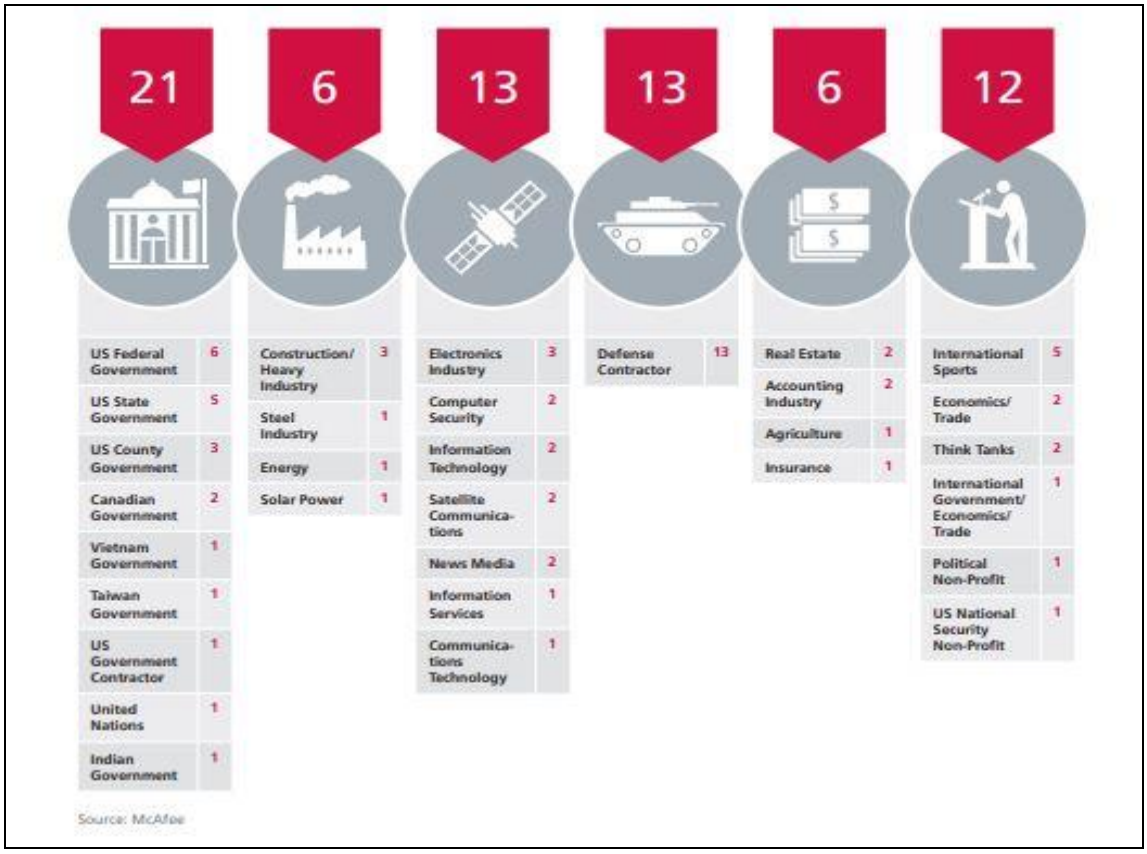
[47] *Hürriyet*. (2012, Aralık 25). Temmuz 5, 2014 tarihinde Hürriyet Gazetesi: http//hürarsiv.hürriyet.com.tr/goster/show new.aspx?id=22229501

[48] McAfee (2011), "Revealed: Operation Shady RAT", http://www.mcafee.com/us/resources/ white-papers/wp-operation-shady-rat.pdf (19.02.2016).

[49] https://nakedsecurity.sophos.com/2011/08/03/shady-rat-biggest-cyber-attack/ Erişim Tarihi: 13/11/2019

[50] https://siberbulten.com/makale-analiz/gelmis-gecmis-en-genis-capli-siber-saldiri-shady-rat/ Erişim Tarihi: 13/11/2019

Şekil 2.7'de Shady Rat saldırısından etkilenen ve kategorize edilebilen kuruluşlar gösterilmiştir. Sınıflandırılması yapılmayan çok fazla hedefin olduğu da raporda yer almaktadır. Kurbanlar arasında sanayi, elektronik, enerji şirketleri-kuruluşları olduğu gibi hükümetlerde yer almıştır.



Şekil 2.7. Shady Rat saldırısından etkilenen organizasyonlar Kaynak: McAfee (2011)

Raporun yazarı Dmitri Alperovitch, 'akla gelebilecek tüm sektörlerde önemli büyüklükteki ve değerli fikrî mülkiyeti ile ticari sırları olan bütün şirketlere sızıldığına (veya sızılacağına) ikna olmuş durumdayım' sözleriyle siber tehditlerin ulaştığı boyut hakkında ilgilileri uyarmaya çalışıyor. Raporda yer alan;

*"*Bu, sayısız ülkenin ekonomisinin hemen hemen her endüstrisini ve sektörünü etkileyen büyük çapta bir sorundur ve bu tehditten muaf olan tek kuruluş, çalmaya değecek değerli ya da ilginç hiçbir şeye sahip olmayanlardır.*"* ifadeleri ile etkilenen aktörlerin bilinenden çok daha fazla olduğunu ve her sektörün siber saldırıların hedefi olabileceğini göstermiştir.

2.3.3.3. Manas üssü süreci -2009

Rusya'ya ait askeri üssün bulunduğu Kırgızistan'da ABD de askeri üs kurmak istemiştir. Terörle mücadele amacıyla dünyanın birçok bölgesinde askeri üs açan ABD Bu üslerden

birisini de Kırgızistan'nın başkenti Bişkek yakınlarında Manas ismiyle kurmuştur. Zamanla Rusya ABD nin bölgedeki varlığından rahatsızlık duymuş ve 2009 yılına gelindiğinde Rusya, ABD'nin bölgedeki politikalarından ciddi bir şekilde rahatsızlık duymuş ve üssün kapatılması için Kırgızistan'a baskı uygulamıştır.[51]

Kırgızistan Manas askeri üssünün kapatılarak 6 ay içinde boşaltılması konusunda parlamento kararı alırken diğer taraftan ABD ile müzakerelere açık olduğunun sinyallerini de vermiştir. Müzakerelerin ardından Kırgızistan'ın internet servis sağlayıcıları siber saldırıya maruz kalmıştır. Saldırılar nedeniyle internet servis sağlayıcıları Batı Kırgızistan'ın %80'ine internet hizmeti verememiştir.[52]

Kırgızistan'a yapılan saldırıların müzakerelerin hemen ardından gelmesi, saldırı şüphesinin ABD askeri üssünün kapatılmasını isteyen Rusya üzerinde yoğunlaşmasına neden olmuştur. Siber güç uluslararası politikanın da yaptırım gücü haline gelmiştir.

2.3.3.4. OpIsrael operasyonu 2012-2013

Anonymous, İsrail hükümetine ait Ağ sitelerini hedef alan kapsamlı bir saldırı düzenledi. İsrail'in Gazze'ye yaptığı askeri operasyonu *"*OpIsrael*"* adını verdikleri, İsrail'e yönelik saldırılarına Kasım 2012'de başlamıştır. Ulusal Siber Büro tarafından yapılan açıklamada, saldırganların önemli sitelerin çoğunu kapatmayı başaramadığını belirtti. İsrailli yetkililerce yapılan açıklamada, 'Şu ana kadar beklenen oldu, hasar yok gibi. Anonymous'un ülkemizin hayati altyapısına zarar verecek becerisi yok. Zaten niyetleri bu olsaydı saldırıyı düzenleyeceklerini günler öncesinden duyurmazlardı. Tek istedikleri medyanın yakından takip ettikleri konularda gürültü yaratmak' denildi.[53] Fakat çok sayıda sitenin erişime engellendiği bilinen bir gerçektir.[54]

7 Nisan 2013 tarihinde İsaril'e *"*OpIsrael*"* operasyonunun devamı niteliğinde büyük bir siber saldırı yapacağını duyurmuştur. "OpIsrael" adıyla başlattığı siber saldırının hedefinde İsrail Savunma Gücü'nün (IDF-Israel Defense Forces) ve İsrail'in önemli kuruluşlarının siteleri olmuştur. Zaman zaman İsrail'in web sitelerine saldırıları devam etmiştir. İsrail'in,

[51]https://21yyte.org/tr/merkezler/bolgesel-arastirma-merkezleri/orta-asya-arastirmalari-merkezi/dar-alanda-buyuk-pazarlik-kirgizistanda-abd-ile-rusyanin-us-mucadelesi Erişim Tarihi: 13/11/2019

[52] 5. Boyutta Savaş: Siber Savaşlar-II, https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html

[53] *Hürriyet*. (2013, Mart 06). Temmuz 1, 2014 tarihinde Hürriyet Gazetesi: http://hurarsiv.com.tr/goster/ShowNet.aspx?id=22749145

[54] Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and cyberspace: Unique threat and response. International Studies Perspectives, 17(3), 307-321.

Kasım 2012'de Gazze'de yürüttüğü operasyonlar neticesinde, İsrail yetkililerinin yaptığı açıklamalara göre İsrail'in web sitelerine karşı 44 milyon siber saldırı gerçekleşmiştir.[55]

İsrail devletinin politikalarına dünya kamuoyunun dikkatini çekmek için tepkiler internet aracılığıyla yapılmıştır. Siber uzayın getirmiş olduğu iletişim ağının büyüklüğü bireylerin tepkilerinin daha farklı boyutlarda göstermesine olanak tanımıştır. Örneklemelerini verdiğimiz çoğu büyük saldırını arkasında bir devlet olduğu düşünülürken bu örnekte saldırı hacker bir grubun organizesinde dahi olsa bireysel tepkiler barındırmaktadır.

2.3.3.5. Ülkeler arası siber saldırılar

Pakistan ve Hindistan arasında Keşmir sorunu nedeniyle ortaya çıkan sorun ülkelerin hackerlarının da katılmasıyla siber saldırılar boyutunda gerçekleşmiştir. Pakistan taraftarı hacker'lar iki ülke arasındaki sorunu tüm dünyaya duyurmak için Hindistan için önemli olan Hindistan Parlamentosu web sitesi, Atom Araştırma Merkezi ve Hindistan Bilim Enstitüsü gibi sitelere saldırmıştır. Hindistan taraftarı hacker'lar da dünya komuoyunda kendilerinin haklı olduğunu göstermek için Pakistan'a siber saldırıda bulunmuşlardır. (Gürkaynak & İren, 2011)

Türkiye-Rusya: 14 ve 24 Aralık 2015 tarihlerinde Türkiye, tarihinin en büyük siber saldırılarına maruz kalmıştır. İnternet hizmetinin engellenmesi amacıyla 6 ayrı DNS sunucularına Siber saldırılar yapılmış ve bu saldırılar neticesinde 400 bin sitede 1 hafta boyunca sorunlar yaşanmıştır. Hacker grubu Anonymous saldırıları üstlenmesine rağmen, böyle büyük çaplı bir saldırıyı tek başına yapamayacağını savunan uzmanlara göre ise bu saldırıların arkasında bir devlet desteğinin bulunması büyük bir ihtimaldir. Siber saldırıların 24 Kasım 2015 tarihinde Rusya ile yaşanan uçak krizi sonrası meydana gelmesi sebebiyle saldırıların arkasında Rusya'nın olması ihtimalini doğurmaktadır.[56]

Çin-ABD: Çin'in güneyinde ABD'ye ait bir keşif uçağıyla Çin uçağının çarpışması sonucu meydana gelen olay siber gerilime neden olmuştur. Siber gerilim olayından sonra bazı Çinli siber saldırganlar ABD hükümet sitelerine uzun süreli yoğun bir saldırı başlamıştır. Saldırıların Çin'den yapıldığı tespit edilmiş ve saldırıları gerçekleştirenler ise Amerika'da Beyaz Saray, Enerji Bakanlığı gibi sitelerin de içerisinde bulunduğu yaklaşık 1200 siteye

[55] Anonymousdeclares"cyberwar"onIsrael, http://edition.cnn.com/2012/11/19/tech/web/cyberattack-israel anonymous/index.html Erişim,08/05/2013

[56] Arslan, Rengin (2015), "Türkiye'ye Siber Saldırının 10 Günü: Ne Oldu?", BBC Türkçe, http://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan (06.02.2016).

saldırı düzenlemişlerdir. (Gürkaynak & İren, 2011) The NewYork Times gazetesi ise bu olayı Birinci İnternet Savaşı (World Wide Web War I) olarak nitelendirmektedir.[57]

2.3.3.6. BlackEnergy ve KillDisk truva atı (2014)

BlackEnergy Truva atı, 2007 yılında bir DDoS hedefli saldırılarda tespit edilen, 2014 yılına gelindiğinde ise yerleştirildiği bilgisayarların sabit sürücülerinden veri toplama, ağ keşfi yapma ve bilgisayarın uzaktan kontrol edilmesini sağlayan bir zararlı yazılımdır. Çoğu Ukrayna'da olmak üzere Polonya'daki birçok devlet kuruluşunun, özel kurumların ve sivil organizasyonların bilgisayarlarında da görülmüştür.

Ayrıca 23 Aralık 2015 tarihinde Ukrayna'da yaklaşık 800 bin kişiyi elektriksiz bırakan enerji dağıtım şirketlerine yapılan siber saldırılarda da BlackEnergy ile birlikte KillDisk Truva atının kullanıldığı belirtilmiştir.[58] KillDisk Truva atı, sistem dosyalarını silmesinin yanı sıra tam bir yok edici olarak çalışmakta, kritik sistemleri kapatan bir zararlı yazılımdır.

Elektrik sistemlerine dahi zarar verecek boyuta gelen siber tehditlerin zararı öngörülemeyecek olabilmektedir. Bu sebeple boyutları savaşın verdiği etkiye eş değer hale gelen siber tehlike tedbirlerini alınması gereken çok ciddi bir güvenlik sorunu haline gelmiştir.

[57] Smith, Craig S. (2001), "6-12; The First World Hacker War", The New York Times, http://www.nytimes.com /2001 /05/13/weekinreview/may-6-12-the-first-world-hacker-war.html (01.02.2019).
[58] Ukrayna Elektriğine Siber Saldırı-Enerji Günlüğü (2016) http:// enerjigunlugu.net/ukrayna-elektrigine-siber-saldiri_16907.html

3. SİBER GÜVENLİĞE İLİŞKİN KAVRAMLAR

3.1. Siber Terörizm Tanımı ve Örnekleri

Türk Dil Kurumu'na[59] göre Türkçedeki karşılığı korkutma, yıldırma, tedhiş " olan "Terör" sözcüğü, Latince "korkudan sarsıntı geçirme, korkudan dehşete düşmeye sebep olma" anlamlarına gelen "terrere" sözcüğünden gelir. Kavram olarak ilk kez Dictionnarire de l'Academı ia Française'in 1789 yılında yayınlanan rastlanmaktadır ve "terör sistemi; rejimi" olarak tanımlanır. Nitekim 1789 Fransız ihtilali sonrasının dönemi tarihçilerince "terör rejimi-rejime de la terreur" olarak anıldığı bilinmektedir. (TBB Raporu, 2006)

3713 sayılı Terörle Mücadele Kanununun 1.maddesinde "Terör" aşağıdaki şekliyle tanımlanmıştır.

> Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.

Terörizm, terör yöntemlerinin siyasi bir amaçla, örgütlü, sistemli ve sürekli bir biçimde kullanılmasını benimseyen bir strateji olarak, terör kavramını da içeren çerçeve bir kavramdır. Emniyet Genel Müdürlüğü terörizmi "Savaş ve diplomasi ile kazanılmayan sonuçları elde etmek, korkutmak ve itaat ettirmek için bir teoriye, felsefeye ve ideolojiye dayanılarak siyasi maksatlarla iradi olarak terör ve şiddetin sistemli ve hesaplı bir şekilde kullanılmasıdır." şeklinde tanımlamıştır. (Gençtürk, 2012)

Siber terörizm ise ekonomik, politik, ideolojik amaca ulaşabilmek için siber uzay elemanlarının, bilgisayar sistemlerinin-ağlarının bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılması olarak tanımlanabilir. (Sağıroğlu, 2017)

Çitlioğlu siber terörizmi;

> Sınırlı insan kaynağı ile en ucuz şekilde yapılan, pek çok hedefi aynı anda etkileyebilmekle birlikte; iletişim olanaklarının gelişmişliğine paralel olarak, büyük organizasyonlar gerektirmeyen, yüksek mobilite ve hızlı reaksiyon yeteneğine sahip, asimetrik olması sebebiyle kaynağında yok edilmesi son derece zor; bağlantılarının kanıtlanmaması ve gizliliği açısından bir devlet ile ilişkilendirilmesi neredeyse

[59] http://sozluk.gov.tr/ Erişim tarihi: 19/07/2019

imkânsız, ulusal ve uluslararası hukuktaki boşluklardan faydalanan modern savaş tekniği

olarak tanımlamıştır. (Çitlioğlu, 2008)

Yapılan tanımlara göre siber terörizm ve klasik terörizm amaç, güdü, ideoloji, sonuçlar vb. fikirsel boyutlarda benzerlik göstermekle birlikte siber terörizmi klasik terörizm tanımından ayıran noktalar vardır.

- Terör eylemleri sırasında terörist unsurlar fiziksel olarak eylemde bulunmaları sebebiyle yaşam tehlikesi ile karşı karşıya gelirken, siber terörizmde böyle bir tehlike yoktur.
- Saldırıların amacı doğrudan zarar vermek olması, fiziksel boyutu olması sebebiyle eylemler araç iken siber terörizmde ise şiddet amaç haline gelmiştir.
- Eylemlerin hızı ve yarattığı etki alanı klasik terör eylemelerine göre siber ortam sayesinde katbekat artmıştır.
- Siber terör saldırıları klasik terör eylemlerine göre daha az toplumsal tepki yaratmaktadır.
- Klasik terörizmin insan kaynağının gerçekleştirilecek eyleme göre yaş, cinsiyet vb. şekilde sınırlılıkları varken, siber terör saldırılarında teknik bilgi dışında hiçbir sınırlılık yoktur.
- Siber terörizmde ihtiyaç duyulan tek teçhizat bir bilgisayar ve internet ağı iken, klasik terörizmde ihtiyaç duyulan teçhizatlar çok çeşitlidir.
- Siber terörizm klasik terörizme göre çok ucuzdur ve daha az risklidir.
- Amaç doğrultusunda oluşturulacak büyük organizasyonlara siber terörizmde ihtiyaç duyulmamaktadır.
- Siber terörizm saldırıların klasik saldırılara göre zaman, mekân ve hedef sınırlılıkları yoktur.
- Klasik terörizmde eylemler propaganda aracı olması sebebiyle saldırıların bağlantıları açık iken, siber terörizmde kişiler ve gruplar anonimlik ve gizlilik esaslı faaliyet yürütürler.

Farkların temelinde yatan ana unsur siber uzayın getirmiş olduğu hız ve gizlilik ve uluslararası hukukta bulunan boşluklardır. Terörizmin siber uzayın yetenekleriyle donanmış halidir siber terörizm.

Yukarıda yer alan çok sayıda sebep ve esasında hızlı sonuç alma ve geniş propaganda imkânı klasik terör yöntemlerini kullanan örgütleri dahi siber alana yönlendirmiştir. Terör örgütleri gelişen teknolojinin imkânlarından yararlanma yoluna gitmişler ve özellikle sosyal medya aracılığıyla propaganda, manipülasyon, algı yönetimi ve dezenformasyon faaliyetlerinde bulunmaktadırlar. (Kartal, 2014, s. 39-77) El Kaide'nin kredi kartı bilgilerinin ele geçirilmesi ile finansal kaynak elde etmesi, IŞİD'in hazırladığı şiddet içerikli videolar ile yakınlıkduyar ve üye devşirmesi bu duruma örnek verilebilir. (Keleştemur S. , 2018, s. 28-32)

Siber uzayda meydana gelen saldırıların ayrımının gizlilik ve bağlantıların tespitinin zor olması nedeniyle net olarak yapılamaması dolayısıyla hangi saldırıların Siber Terörizm olduğu tartışılan bir konudur. Siber terörizm oldukları yönünde genel kabul gören örnekler aşağıdaki şekilde sıralanabilir: (Yalman, 2018, s. 259)

- 1991: 1. Körfez Savaşı esnasında Hollandalı bir grup saldırgan Pentagon merkezi bilgisayar sistemine sızarak ABD'nin savaş operasyonlarını değiştirmiş ve mevcut planları kopyalanması,
- 1996: CIA'nin internet sayfasına gerçekleştirilen saldırılar sonucunda, sayfadaki bilgiler değiştirilmesi,
- 2001: California elektrik hizmet sağlayıcısına yapılan saldırı sonucu internet 1 gün süre ile kesilmesi,
- 2014: Rusya kaynaklı olduğu iddia edilen ve Ukrayna'da internetin kesintiye uğratılması ile Rusya yanlısı isyancıların Kırım'ın kontrolünü ele almasını destekleyen bir DDoS saldırıları,
- 2014: Ukrayna Cumhurbaşkanlığı seçiminden 3 gün önce Rusya'da bulunduğu iddia edilen bir grup saldırgan tarafından seçim komisyonu sistemi hedef alınıp sistemin işlevsiz hale getirilmesi,
- 2014: 500 milyon Yahoo kullanıcısının şifreleri çalınmış olup, ilgili şifrelere ek olarak kişisel bilgiler ile gizli soru-yanıtlarının da çalındığı şirket tarafından kabul edilmiştir. Daha önce de MySpace'in 359 milyon, LinkedIn'in 159 milyon ve Adobe'un 152 milyon kullanıcısına ait bilgiler çalınmıştır.
- 2015: Saldırganların Alman politikacılar tarafından kullanılan 20 bin bilgisayarı etkileyerek, hassas verileri çalmış ve karşılığında milyonlarca avro istemeleri,

- 2016: Bir grup siber saldırgan tarafından Ukrayna'daki 3 bölgesel elektrik şirketine yapılan DDoS saldırısı sebebiyle 225.000 müşterinin elektrikleri kesintiye uğratması ve bu saldırıların aynı zamanda telefon hatlarını da kullanılamaz hale getirmesi,
- 2017: Dünya genelinde hastaneler, devlet daireleri WannaCry isimli sızdığı bilgisayarlarda veya sistemde verilere ve tüm sisteme erişimi engelleme yoluyla fidye talep fidye yazılımı sebebiyle çok zor durumda kalmıştır. Bu virüs fidye karşılığında ele geçirdiği dosyaların iade edilmesini sağlayan bir algoritma ile çalışmaktadır. 99 ülkede 75.000 civarında fidye saldırısı olduğu rapor edilmiştir.

Bu saldırılar saldırganların maddi çıkar amacı sebebi ile Siber Suç olarak değerlendirilebilirken, kullanıcılar üzerinde oluşturduğu korku, sistemlerin çalışamamasını sağlaması gibi sebeplerle Siber Terörizm olarak da nitelenebilecek bir olaydır.

Her siber saldırı-suç siber terörizm faaliyeti olarak değerlendirilemese de; siber terörizm faaliyetleri birer siber suç olarak değerlendirilmektedir. Siber terörizm ise belirli olgulara sahip olması gerekmesi sebebiyle daha spesifik bir suç faaliyetidir.

3.2. Siber Savaşın Özellikleri ve Örnekleri

İnternetin ortaya çıkması, bilişim sistemlerinin hızlı bir şekilde yayılması sonucu ekonomik alandan askeri alana kadar hemen hemen her şey dijitalleşmiş ve etkileşime açık hale gelerek güvenli olmaktan uzaklaşmıştır.

Tarih boyunca yapılmış olan birçok savaşın geri planındaki sebebi aslında karşı taraftan bilgiyi çalmaktır. Rakip devletlerin çıkarları doğrultusunda birbirlerine siber savaş başlatması olağandır, devletlerin bundan bilgisi olmamasına rağmen, bu savaşlar gerçekleşir ve çıkarları doğrultusunda ele geçirilen bilgiler kullanılır, değiştirilir veya ifşa edilir. Coşkun'a göre Siber Savaş; (Coşkun, 2018)

"Varlığı bilinen ancak etkisi görülmeden farkına varılmayan sessiz bir savaştır."

Hedef ülkeye ekonomik, politik veya askeri nedenlerle, bilgi sistemleri ve ağları kanalıyla gerçekleştirilen organize saldırılara ve ülkede sivil, askeri ve hükümete ait kritik yapıların bilgisayar sistemlerinin ve ağlarının siber saldırılara karşı savunulmasına, siber savaş denir. (Yazıcı, 2011) Gizlilik dereceli bilgilerin ele geçirilmesi, kritik alt yapılar olan enerji-iletişim-güvenlik altyapıları gibi sistemlere yönelik saldırılar, internet üzerinden propaganda ve Web sayfalarının ele geçirilmesi siber savaşta yapılabilecek başlıca saldırılardır. (Üneri, 2009)

Siber uzayda, ağ ve internet üzerinden bir kurum veya devleti

- ❖ Maddi ve manevi zarar vermek,
- ❖ Altyapı sistemlerine sızarak çalışamaz hale getirmek,
- ❖ Rakip devlet aleyhinde kamuoyu oluşturmak,
- ❖ Gizli bilgi elde etmek

gibi sonuçları elde etme amacıyla sistematik bir şekilde saldırıya maruz bırakmak suretiyle ortaya çıkarılan duruma siber savaş denir (Şahinaslan, 2013).

Kara, hava, deniz ve uzaydan sonra 5. Boyut savaş alanı olarak kabul edilen Siber Savaş, rakip devletleri psikolojik olarak çökertmek için internet ağındaki bilişim sistemlerine izinsiz ve gizli olarak erişmek, kontrolü ele geçirerek bilgileri çalmak, değiştirmek, çökertmek ya da yanlış yönlendirmektir (Kara, 2013).

Konvansiyonel Savaş ile Siber Savaş Arasındaki Farklar

KRİTERLER	KONVANSİYONEL SAVAŞ	SİBER SAVAŞ
Saldırı Kaynağı	Saldırının kaynağının tespiti kolaydır.	Saldırının nereden geldiğini tespit etmek zordur. Bazen de imkânsızdır.
Saldırının Hızı	En hızlı muharebe silahı hızındadır.	Işık hızındadır.
Saldırının Etkisi	Çoğunlukla fiziksel alanda etkilidir	Çoğunlukla bilgi ve iletişim sistemleri alanında etkilidir.
Savaşanlar	İki veya daha fazla ülke orduları savaşmaktadır.	Tek bir kişi, bir grup, bir örgüt veya devletler savaşmaktadır.
Maliyeti	Oldukça pahalıdır.	Genelde ucuzdur.
Kullanılan Silahlar	Tank, top, tüfek, füze, bomba, uçak, gemi, füze, radar vb. kullanılır.	Bilgisayarlar, bilgi sistemleri vb. kullanılır.
Teknoloji İhtiyacı	Genelde ileri teknoloji gerektirmektedir	İleri teknolojiye ihtiyaç duyulmamaktadır. Mevcut teknoloji genellikle yeterlidir.
Saldırının Belirtileri	Saldırının farkına varılır.	Saldırının farkına varılmayabilir.
Hasar Tespiti	Nispeten kolaydır.	Zordur. Çoğu zaman imkânsızdır.

Tablo 3.1. Konvansiyonel savaş ile siber savaş arasındaki farklar (Çifçi, 2013) (Keleştemur A. , 2015)

Siber savaşı diğer savaşlardan ayıran temel unsurlar 2010 yılında yayınlanan "Chatham House Report" da aşağıdaki başlıklar altında sıralamıştır. (Cornish, Livingstone, Clemente, & Yorke, 2010)

- ❖ Aktörlerin silahlı çatışmalara ihtiyaç duymadan siyasi ve stratejik hedeflerine ulaşmalarını sağlayabilir.
- ❖ Küçük ve önemsiz aktörlere orantısız güç imkânı verir.

- ❖ Sahte IP adresleri ve yabancı sunucuların ve takma adların arkasında faaliyet göstererek kısa vadede anonimlik sağlayabilirler.
- ❖ Siber savaş konvansiyonel savaştan farklı olarak siber uzay olarak tanımlanan beşinci boyutta icra edilir.
- ❖ Klasik savaş çatışma ve baskı rejimi gibi unsurlardan sonra ortaya çıkması olası iken siber savaş fiziksel baskı ve çatışma ortamından uzaktır.
- ❖ Siber savaşta askeri ve sivil, fiziksel ve sanal, devlet ve devlet dışı aktörler arsında güç kullanımı sınırları belirsizdir.

Siber savaşın klasik konvansiyonel savaşın yerini almasında ülkelerin çıkarları doğrultusunda teknolojiyi silah olarak kullanması etkili olmuştur. Konvansiyonel savaş ile siber savaş arasındaki farklar ve siber suç, siber saldırı ve siber savaş özelliklerini içeren karşılaştırmalı bilgiler aşağıdaki tabloda belirtilmiştir.

Siber suç, siber terör ve siber savaşın temel özellikleri;

Eylemin	Siber Suç	Siber Terör	Siber Savaş
Niteliği	Doğrudan	Doğrudan, Sembolik	Doğrudan, Sembolik
Şiddeti	Az Yoğun	Yoğun	En Yoğun
Motivasyonu	Kişisel Kazanç	Siyasi	Siyasi, Doğrudan Savaş Kabiliyetini Azaltmak, Casusluk
Failleri	Bireyler, Organize Suç Örgütleri, Anonim	Terörist Örgütler, Hangi Örgüt Olduğu Tahmin Edilebilir.	Failin kim olduğu tam olarak bilinmese de hangi devletlerden kaynaklandığı bilinebilir.
Hedefleri	Kazanç Sağlanacak Hedefler	Kritik Tesisler, Güvenlik Birimleri, Hükümet Temsilcilikleri	Kritik Tesisler, Ekonomik ve Endüstriyel Altyapılar, Güvenlik Birimleri, Hükümet Temsilcilikleri, Askeri Altyapılar.
Kaynağı	Ülke İçinden veya Dışından	Ülke İçinden veya Dışından	Ülke Dışından

Tablo 3.2. Siber suç, siber terör ve siber savaşın temel özellikleri (Ercan, 2015)

Geçmişten günümüze resmi olarak sava olarak nitelendirilmese dahi siber güvenlik alanında yapılan çoğu çalışmada sava olarak kabul görmüş çeşitli yaşanmış siber savaş örnekleri mevcuttur.

3.2.1. Sibirya Doğalgaz Patlaması-1982

Sibirya Doğalgaz Patlaması1982 yılında gerçekleşen ilk siber savaş örneğidir. ABD ve Rusya arasında yazılım çalınması sonucu meydana gelmiştir. Moskova, Kanadalı bir şirketten doğal gaz boru hatlarını kontrol etmeye yardımcı olacak bir yazılım çaldı. Kısa süre

içerisinde bu durumu fark eden ABD yazılımın içerisine kendi lehlerine kullanabilecekleri bir virüs yerleştirdi. Rusların fark edemediği böcekli yazılım boru hatlarındaki akışı normalin dışında seviyelere çıkarttı. Bu normal olmayan seviyeler sonucunda borular infilak etti ve uzaydan dahi görülebilecek bir patlamaya neden olundu (Karakuş, 2019).

3.2.2. ABD-Irak Savaşı

1992 Yılında ABD, Irak savaşı başlamadan önce ABD tüm iletişimi tek bir kodla sonlandıracak siber savaş tertip etti. Savaşın başlaması ile tüm iletişimi tek bir kod satırıyla sonlandırmıştır. Irak'ta meydana gelen bu iletişim çöküşü askerlerin arasındaki irtibatı en aza indirgemiş ve savaşın doğrudan ABD'nin lehine sonuçlanmasına yardımcı olmuştur (Karakuş, 2019).

3.2.3. Estonya Siber Savaşı

2007 yılında NOTO ülkesi Estonya'nın maruz kaldığı siber saldırı ise hazırlık boyutunu farklı bir seviyeye taşımıştır. Rusya'nın İkinci Dünya Savaşı esnasında Estonya'ya Nazi istilasından korunmayı simgeleyen bir heykel dikmiştir. 26 Nisan 2007 tarihinde Estonyalı yetkililer bu heykeli kaldırmıştır. Siber saldırılar hemen bu heykelin kaldırılmasının ardından gerçekleşmiştir. Ülkenin internet hizmet sağlayıcıları, bankaları, bilgi sistemleri bu saldırılar neticesinde ciddi zararlar görmüştür. Ülkenin internet sistemi neredeyse tamamıyla çökme tehlikesiyle karşılaşmıştır. Estonya siber saldırının esiri olmuştur (Bakır, 2011).

30 Nisan-18 Mayıs tarihleri arasında ise saldırılar hedefini daha organize hale getirmiştir. Ulusal bilgi sistemleri, internet hizmet sağlayıcıları büyük zararlar görmüştür. İletişim ve ticaret durma noktasına gelmiştir. (A.Clarke & Knarke, 2011) Estonya saldırılar ile ilgili Rusya'yı suçlasa da, Rus yetkililer söz konusu siber saldırıların kendileri ile ilgisi olmadığı konusunda ısrarcı olmuşlardır (Bakır, 2011).

Estonya'nın web sitelerine düzenlenen saldırıda Estonya Meclisinin sitesine, tüm bakanlık, siyasi parti, en büyük bankaların ve altı büyük haber kuruluşunun sitelerine, ana hedef olarak saldırılmıştır (Traynor, 2019).

3.2.4. Suriye-İsrail Gerginliği -2007

Nükleer tesis olduğu zannedilen ve Türkiye'nin Suriye sınırından yaklaşık 120 km içerde olan bir binayı İsrail uçakları, 6 Eylül 2007'de, bombaladı. Suriye'nin ancak sabah haberi oldu. Suriye'nin Rusya'dan satın almış olduğu radarların İsrail uçaklarının hava sahasına girişini görüntülemiş olması gerekirdi. Yapılan soruşturmanın ardından İsrail'in Suriye

savunma ağına yerleştirdiği zararlı bir yazılım sayesinde radarlardaki görüntüyü silerek yerine boş bir hava sahası fotoğrafı yerleştirmiştir. Suriyeli askeri yetkililer 06 Eylül 2007 gecesi tertemiz bir radar görüntüsü izlemişler ve sorunsuz bir gece geçirdiklerini düşünmüşlerdir (A.Clarke & Knarke, 2011).

3.2.5. Rusya – Gürcistan Vakası-2008

2008 yılında Rusya ile Gürcistan arasında Güney Osetya yüzünden çatışmalar çıkmış. Rusya, Gürcistanın bilgi ve iletişim teknolojileri ile kritik altyapı sektörlerine karşı yoğun bir şekilde siber saldırılar başlamıştır. siber saldırı yöntemleri arasında Estonya örneğinde olduğu gibi DDoS saldırıları bulunmaktadır. (Çifçi, 2013) Bu saldırılarda Gürcü medyası ve kamu internet sayfaları zarar görmüş ve sonucunda da Gürcistan'ın dış dünya ile bağlantısı kopartılmıştır. Enformasyon altyapısının çok gelişmiş olmaması ile bilgi ve iletişim teknolojilerinin internete aşırı bağımlılığı olmadığından Gürcistan, bu saldırılardan az zararla çıkmıştır. Gürcistan olayının en önemli özelliği, konvansiyonel savaş yöntemlerinin yanında siber silahların da kullanılması sebebiyle operasyonel siber savaş örneği teşkil etmesidir (Aydın, 2013).

Gürcistan ve Rusya arasındaki siber savaş kamuoyunu şekillendirme maksadı da taşımaktadır. İki tarafça da gerçekleştirilen *DoS* saldırılarına ilave olarak sahte siteler oluşturulmuş, bu sitelerde yoğun propaganda faaliyeti gerçekleştirilmiştir (Gürkaynak & İren, 2011).

Yukarıda yer alan sınırlı örnekler ve yaşanmış diğer olaylar göz önünde bulundurulduğunda, siber savaşta neler yapılabileceği aşağıda belirtilmiştir; (Çifçi, 2013)

- Petrol ve Doğalgaz hatlarında, nükleer tesislerde yangın çıkıp patlama olabilir,
- Hava trafik kontrol sisteminde meydana gelen arıza ve hatalı çalışmalardan dolayı uçaklar havada çarpışabilir,
- Elektronik bankacılık durursa bankalar çalışamaz hale gelebilir ve müşteri verileri çalınabilir, silinebilir,
- Bankalardan ve ATM'lerden para çekemeyen vatandaşlar mağaza ve dükkânları yağmalayabilir,
- Metro ve Trenler birbirleriyle çarpışabilir, raydan çıkabilir, hatalı yönlere sevk edilebilir,
- Elektrik dağıtım şebekesine yapılan olası bir saldırı durumunda elektrikle çalışan hiçbir alet kullanılamaz,

- ❖ Trafik ışıkları hatalı bir şekilde çalıştırılarak çarpışma ve tıkanmalar meydana gelebilir,
- ❖ Uydu sistemleri ele geçirilip, meteoroloji, seyrüsefer, iletişim uyduları ve diğer uydular düşürülebilir veya yörüngesinden çıkarılıp rotasından saptırılabilir,
- ❖ İnternete erişim kesilebilir. Bilet ve otel rezervasyonları, banka işlemleri, e-ticaret gibi işlemler kesintiye uğrar.

Yaşanmış olan siber saldırılardan çıkarılacak beş tane ders vardır: (A.Clarke & Knarke, 2011)

1. Siber savaş gerçektir,
2. Siber savaş ışık hızında gerçekleşmektedir,
3. Siber savaş küreseldir,
4. Siber savaş geleneksel savaş alanından önce yer almaktadır,
5. Siber savaş başlamıştır.

3.3. Siber Güvenlik Kavramının Çerçevesi, Yaklaşım Türleri ve Önemi

Güvenlik nedir?

Tarihsel bir geçmişe sahip olan güvenlik, uluslararası boyutta temel unsurların başında gelen yapısıyla farklı değerlendirmelere konu olmuştur. Türk Dil Kurumu'na göre güvenlik, *"*toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*"* şeklinde açıklanmıştır.[60]

Tarihsel süreçte güvenlik algısı iç ve dış güvenlik olmak üzere iki boyutta ele alınmıştır. İç güvenlik algısı asayiş durumunu ifade ederken, dış güvenlik algısı ise sınırlar dışarısından gelebilecek olan olası saldırılar olarak açıklanmaktadır. Güvenlik küresel boyutta devletleri tehdit eden saldırılara karşı vazgeçilmez bir unsurdur.

Realizm ve neo-realizm kuramı güvenlik algısını, askeri güç olarak değerlendirmiştir. Her iki yaklaşıma eleştirel bakan Kopenhag Okulu ise, kapsamlı bir şekilde ele aldığı güvenliğin sosyal, ekonomik, askeri ve çevresel sektörlerine vurgu yapmıştır.

[60] "Güvenlik", Türk Dil Kurumu, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.53ec947c405869.39672886

Realist ve neo-realist yaklaşımlarla güvenlik

Devletin tek hakim aktör olduğu devlet güvenlik anlayışı, Realizmin güvenlik anlayışında etkili görüş olmuştur. Devletin çıkarlarının sağlanması, temel amacın varoluş mücadelesi olduğu şeklinde tanımlanmaktadır.

Devletlerin güç unsuru temel olarak askeri güç olarak tanımlanmaktadır. Dolayısıyla güç faktörleri devletlerin güvenliğini sağlayacak temel unsur olarak öne çıkmaktadır. Devlet bekâsının güç faktörlerine bağımlı olduğu, uluslararası ilkelerin bulunmadığı bir ortamda devletlerin kendi güvenliklerini kendilerinin sağlamasıyla meşrulaşan yüksek düzeyde güç geliştirme ve kullanma durumu, yapının "rekabetçi ve çatışmacı karakterini" ortaya koymaktadır. Bu yapıya uyum sağlayamayan devletlerin ise sistemden dışlanacağı öngörülmektedir. [61]

Realist yaklaşımcılara göre savaşlar, doğal bir durumdur. Devletler, kendi güvenliklerini sağlamak için güvenliği en önemli sorumluluk olarak kabul etmişlerdir. Geçmişte ve günümüzde devletler, eli silah tutan herkesi asker olarak kabul etmiş, devlet güvenliğini bu bağlamda dinamik hale getirmeye çalışmışlardır. Bu durum tarihte Perslerin yurttaşlık ve vatan bilinci ile eli silah tutan herkesi askerliğe alıp "kamu hizmeti" yaptırması, Atina ve Sparta'nın sürekli savaş halinde olması, günümüzde ise az gelişmiş veya gelişmekte olan ülkelerde askerlik hizmetinin zorunlu olması örnek olarak gösterilebilir. (Machievelli (Çev. Nazım Güvenç), 2002)

Görüldüğü gibi realizm güvenliği doğal olarak güç ile ifade etmektedir. Diğer devletlere göre daha baskın yeterli bir güce sahip olan devlet daha güvenli olacaktır. Bu düşünceye göre güvenliğin sağlanmasında askeri faktör esas çözüm yoludur (Alkan, 2006).

Neorealizmin sistemsel yaklaşımına göre, devletlerin bir birlerine benzer davranış ve hareketler gösterdiği sistem içerisinde yapısal ve sonuçsal farklılıklara neden olan temel unsuru devletlerin güç kapasiteleri oluşturmaktadır. Devletlerin güç dağılımındaki farklılıkları sistemin yapısında değişikliklere neden olmaktadır (Arı, 2006).

Neorealist yaklaşımda devletlerarasında işbirliğinin sınırlı bir şekilde gerçekleşeceği ve bu işbirliğinin güvenlik meseleleri üzerinden şekillenip hâkim güvenlik rekabeti mantığına

[61] Alexander Wendt, "Anarchy is What States Make Of It: The Social Construction Of Power Politics",International Organization, 46: 2, 1992, s. 392.

dayanacaktır. Dolayısıyla uzun süreli kalıcı bir barıştan veya güç mücadelelerinden temizlenmiş bir dünyadan söz etmek mümkün değildir (John, 2008, s. 18).

Realist ve neorealistler geçmişte yaşanan savaşların varlığını göz önüne alarak, gelecekte de savaşların olacağı gerçeğini savunurlar. Savaş ihtimali devletlerin güç arayışları içerisinde olduğu gerçeğini belirtmektedirler. Zbigniew Brzezinski "İkinci Şans" adlı eserinde Amerika'nın güç sahibi olmasının devletleri kendi tarafına çekeceğini belirtmektedir. Bu durumda, güç kazanımını etkileyen en önemli faktör ise nükleer silahlanma olarak belirlenmiştir.[62] (Zbigniew Brzezinski (Çev Yelda Türedi) 2008).

Realist ve neorealist anlayışların uluslararası ilişkilere bakışı güç ve güvenlik konuları üzerinden şekillenmektedir. (John, 2008) Realist ve neorealistler dünyayı gördükleri gibi yorumlamaktadır. Devletlerin varlığının devamı için güvenlik her zaman en önemli görevdir. Bu doğrultuda devletlerin birbirleri ile olan ilişkisi sadece çıkara dayalı gerçekleşirken kalıcı bir barışın sağlanmasının zor olduğu belirtilmektedir.

Kopenhag okulu'nun güvenlik anlayışı

Güvenlik yaklaşımını askeri güvenlik üzerine inşa eden ve güvenlik anlayışını devletlerarasındaki güç dağılımına bağımlı kılan realist / neorealist yaklaşıma eleştiri getiren Kopenhag Okulu güvenliğin daha geniş kapsamlı irdelenmesi gerektiğini savunmuştur.

Önemli teorisyenlerden olan Barry Buzan, Kopenhag Okulu'nun önde gelen isimlerinden biridir. 1983 yılında yayınladığı "Halklar, Devletler ve Korku" isimli kitabında askeri güvenlik anlayışına eleştiriler yöneltmiş ve güvenliğin çok dar anlamda tanımlandığını vurgulamıştır. (Alkan, 2006) Güvenlik çalışmalarını savaş kavramı, tehdit ve askeri gücün kullanımı çerçevesinde değerlendiren gelenekçiler karşısında Buzan "genişletilmiş güvenlik" kavramını ortaya koymuştur. Buzan güvenliği askeri, siyasi, ekonomik, sosyal (toplumsal) ve çevresel olmak üzere beş ayrı sektörde incelemektedir. (Buzan, 1991)

Kopenhag Okulu'nun önde gelen isimlerinden Ole Waever, güvenliğin üç temel konu üzerinde şekillendiğini belirtmektedir. Bunlar; sektörler, güvenlikleştirme ve bölgesel güvenlik yapılanmalarıdır (Weaver, 2004) devlet odaklı askeri güce bağımlı anlayışın ilerisine geçerek çok boyutlu bir yaklaşımla sektörler bazında incelenmektedir.

[62] Zbigniew Brzezinski, "İkinci Şans", (çev.: Yelda Türedi), İkılap Yayınevi, İstanbul 2008, s. 40-41.

Kopenhag Okulu'nun üzerinde durduğu diğer bir önemli konu bölgesel güvenlik yapılarıdır. Barry Buzan bölgesel güvenlik yapılarını bir grup ülkenin temel güvenlik kaygılarının, gerçekçi bir şekilde birbirinden ayrı düşünülemeyecek kadar birbirine bağlanması şeklinde tarif etmektedir (Buzan, 1991).

İdealist teori'de güvenlik algısı

İdealist düşünürler güvenlik algısını uluslararası barış şeklinde açıklamışlar. Bu nedenle uluslararası barışın sağlanması gerektiğini savunarak bu fikre sıkı sıkıya bağlıdırlar. Uluslararası barışın sağlanması ve devam etmesi için de devletlerin karşılıklı ilişkiler içerisinde olması gerektiğini ifade ederler. Ticari ilişkilerin geliştirilmesi gibi menfaate dayalı bağların barış için ön koşul olduğu belirtilmektedir (Sandıklı, Kaya, 2013: 61).

İdealist düşünürler uluslararası politika'da siyasal ve sosyal bir varlık olarak devleti ana aktör olarak görürler (Ateş, 2013:61).

İdealizm'in politikaya bakış açısı daha çok normatif özelliklere sahiptir. İdealistlerin öncülerinden olan Platon, "*politikayı faziletli bir yaşam ve bu yaşamı mümkün kılan toplumsal düzeni sağlayacak bir araç*" olarak görmüştür. Aristo'ya göre eğitimin insanların olumsuz davranışlarını değiştireceğini ve bu sayede iyi insanların varlığının artacağı, buna bağlı olarak da iyi yönetim biçimlerinin ortaya çıkacağı ve tehlikelerden uzak güvenli bir ortamın oluşacağını belirtmektedir (Birdişli, 2011: 153-154).

Soğuk savaş döneminde güvenlik anlayışı

Soğuk savaş dönemindeki güvenlik Geleneksel güvenlik anlayışında olduğu gibi, güvenlik, devlet odaklı olup temelinde askeri tehdit ve riskleri barındıran bir bakış açısına sahiptir.

Bu dönemde ortaya çıkan belli başlı ekoller ve çalışmalar aşağıdaki gibidir.

1) Kritik Güvenlik Çalışmalar

2) Stratejik Çalışmalar

3) Feminist Güvenlik Çalışmaları

4) İnsan Güvenliği

5) Barış Araştırmaları

6) Sömürgecilik Sonrası Güvenlik Çalışmaları

7) Post Yapısalcı Güvenlik Çalışmaları (Buzan, Hansen, 2009:35-37).

Modern anlamda güvenlik yaklaşımı

Modern anlamda güvenlik yaklaşımını dört farklı dönemde meydana gelmiştir. İlk dönem olan 1918-1955 yılları arasında güvenlik daha çok disiplinler arası bir yaklaşım olarak vurgulamış ve silahsızlanmanın sağlanması olarak belirtilmiştir.

İkinci dönem olan 1955-1985 yıllarını kapsayan süreç nükleer silahların uluslararası politikayı yönlendirmeye başladığı dönem olarak belirtilir. Nükleer savaş, sınırlı savaş ve silahların kontrolü gibi yeni konular gündeme gelmeye başlamıştır.

Üçüncü dönem 1985-1995 yıllarında güvenlik anlayışı yeniden tanımlanmaya başlanmış, güvenliğin ekonomik gelişme ve siyasal bütünleşme ile ilişkisi üzerinde durulmuştur.

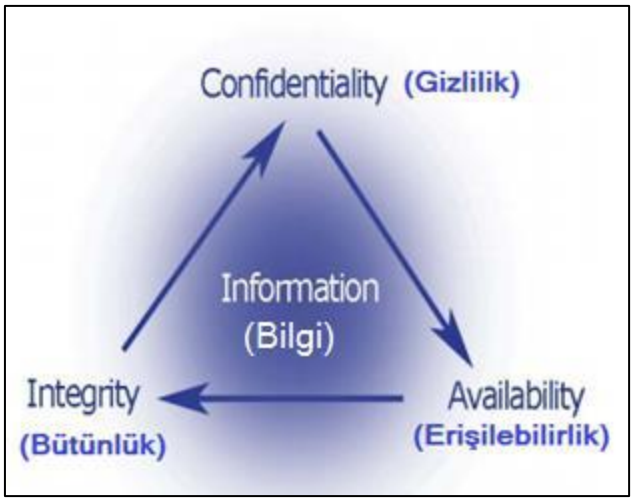
Son dönem ise 1995'ten günümüze kadar olan süreyi kapsayan Eleştirel Güvenlik Çalışmaları adı altında yapılan çalışmalardır. Güvenlik bu dönemde aktör, boyut ve seviyesinin analizi şeklinde cereyan etmiştir (Bakan, 2007: 37-42).

Siber güvenlik alanı ve yaklaşımları

Siber güvenlik; bilgi bileşenlerini ve ağlarını etkisizleştiren veya çalışmaz hale getiren tüm tehdit, saldırı ve tehlikelere karşı teknolojik sistemleri korumaya denilmektedir. (Akleylek ve Tok, 2011). Hansen ve Nissenbaum (2009: 1160) ise siber güvenlik kavramının ilk defa 1990'lı yıllarda bilgisayar mühendisleri tarafından ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek amacıyla kullanıldığını belirtmiştir.

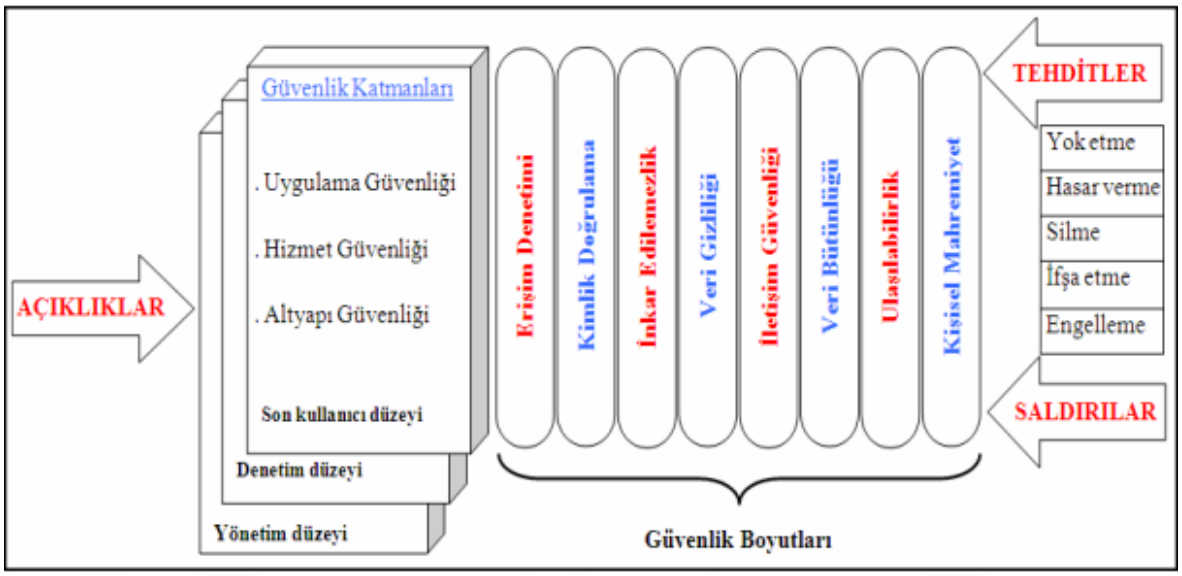
Siber ortamda var olan bilişim teknoloji sistemlerini tehdit ve saldırılardan korumak, korunmak istenen bilginin gizliliğini en yüksek seviyeye çıkarmak, saldırı ve tehditlerin kaynağını tespit etmek ve karşı hamleler geliştirmek amacıyla oluşturulmuş olan ulusal hukuk, uluslararası hukuk ve insan haklarına uygun her türlü önlem ve sistemleri siber güvenlik olarak tanımlayabiliriz (Kara, 2013: s. 5-6).

Siber ortamı oluşturan bilişim sistemlerinin tehdit ve saldırılara karşı korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırı tehdit ve siber güvenlik olaylarının tespit edilmesi ve karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder.



Şekil 3.1. Siber uzayın güvenlik bileşenleri

Siber güvenlik kavramı üzerinde de kavramsal olarak uzlaşı sağlanmamış olmakla birlikte, literatürde bilgi güvenliği (information security) ve bilgisayar güvenliği (computer security) kavramları ile ilişkili olarak kullanılmaktadır. Bilgi güvenliği kavramı kişisel ve kurumsal verilerin korunması, bilgisayar güvenliği kavramı ise bilişim sistemlerinin güvenliğini ihtiva eden bir kavram olarak kullanılmaktadır. Siber güvenlik kavramının tanımı, bilişim sistemlerinin temel değeri olan bilgi üzerinden yapılmaktadır. Siber uzayın güvenli olabilmesi için bilgiye dair üç temel hususun sağlanması gerekmektedir. Bilginin gizliliği (confidentiality), bilginin bütünlüğü (integrity) ve erişebilirliği (availability) siber güvenliğin sağlanması için gereken hususlar olarak karşımıza çıkmaktadır (Goodrich ve Tamassia, 2010) Bu üç hususun siber güvenliğin temel hedefleri olduğunu söylemek de mümkündür. (Uluslararası Telekomünikasyon Birliği, 2008)



Tablo 3.3. ITU, "ITU_T X.1205 sayılı tavsiye kararı, siber güvenliğe genel bakış", 2008

Tablo 3.3'te yer alan bilgi güvenliğini en üst seviyede sağlamak maksadıyla, uygulanan söz konusu prensipler aşağıdaki gibi tanımlanabilir:

• *Gizlilik:* Veriye sadece yetkili kişilerin erişilebilmesini ifade eder.

• *Bütünlük:* Verinin, göndericiden çıktığı orijinal haliyle bozulmadan alıcısına ulaşmasıdır.

• *Erişilebilirlik:* Yetkili kişilerin ihtiyaç duyulduğunda ve ihtiyaç duyulan kalitede bilişim sistemlerine erişebilmesi demektir.

• *İzlenebilirlik:* Sistemde gerçekleşen olayların sonradan analiz edilmek için kayıt altına alınmasıdır.

• *Kimlik Doğrulama:* Alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır.

• *Güvenilirlik:* Sistemde beklenen davranışlar ile elde edilen sonuçların birbiri ile tutarlı olmasıdır.

• *İnkâr Edememe:* Göndericinin gönderdiği mesajı, alıcının da aldığı mesajı inkâr edememesidir. (Ada, 2018)

Şekil 3.2. Parker altılısı (Pender-Bey 2012)

Parker altılısında verilen unsurlardan erişebilirlik, gizlilik ve bütünlük yukarıda tanımlanmış olup, özgünlük, yararlılık ve sahiplik/kontrol aşağıdaki gibi tanımlanabilir.

Özgünlük: Doğrulanabilir ve güvenilir olma:

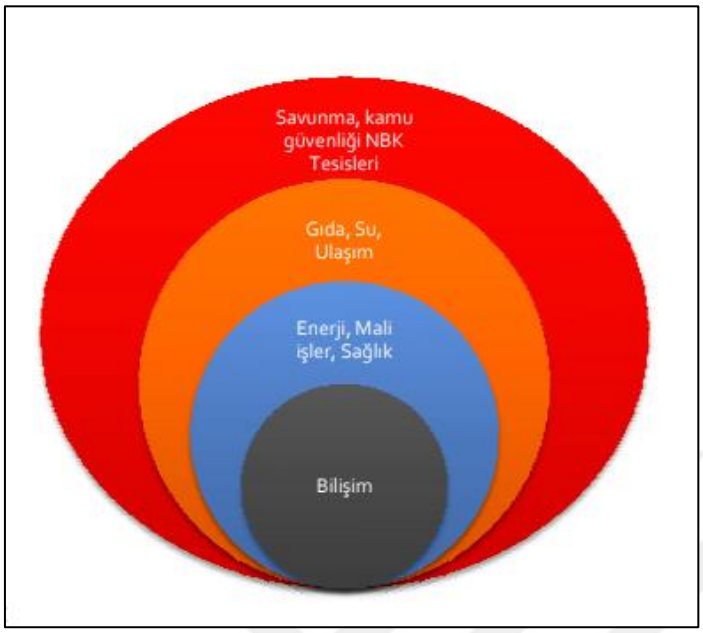
Yararlılık: Amaca uygunluğu ifade eder.

Sahiplik/Kontrol: Bilginin yetkisiz kişilerce kullanılmasını engellemeyi ifade eder.

Siber uzayın güvenliğini sağlamak ve korumak için yapılan çalışmaların tümüne "Siber Güvenlik" adı verilir 2013 yılında yayınlanan Resmi Gazetede "Bilişim Güvenliği", "dijital ortamda depolanan bilgilerin üçüncü şahıslar tarafından ele geçirilmesini önlemek, bilgi transferi sırasında bilginin bütünlüğünün ve yapısının bozulmadan aktarılmasını sağlamak, sistemlere yetkisiz kişilerin erişmesini engellemek, sistemin sürekli olarak erişilebilir olmasını sağlamak için verilmesi gereken uğraşların tümü" olarak tanımlanmıştır.

Uluslararası Telekomünikasyon Birliği (ITU) tarafından hazırlanan "ITU-T X.1205: Overview of cybersecurity" standardında belirtildiği şekliyle siber güvenlik, siber kurum-kuruluş ve kullanıcıların güvenliklerini sağlamak amacıyla kullanılabilecek araçlar,

politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplanmasıdır.



Şekil 3.3. Türkiye kritik altyapı sektörleri (Alkan M. , 2012)

Devletlerin temel olarak siber alanında öncelikli olarak güvenliklerini sağlamaları gereken alanlar ise; bilişim, enerji, mali işler, gıda, sağlık, su, ulaşım, kamu güvenliği, savunma, nükleer, biyolojik ve kimyasal tesislerdir. (UDHB, 2012).

Joseph Nye bu noktada devletlerin siber güvenliğine yönelik temel tehditleri;

1. Devletlerin birbirlerine karşı oluşturduğu siber tehditler,

2. Devlet dışı aktörlerin devletlerin siber güvenliğine yönelik tehditler

şeklinde sınıflandırmıştır. (Nye, 2011) Siber güvenliğin sağlanması konusunda ulusal boyutta öncelikli alanları ve diğer bütün bilişim ağının güvenliğinin sağlanması için yapılması gereken çalışmalar aşağıda belirtilen adımlardan oluşmaktadır.

Siber güvenliğin unsurları

Şekil 3.4. Siber güvenliğin unsurları (Alkan M. , 2012)

1. Ulusal politika ve stratejinin geliştirilmesi: Bireyler, sivil toplum kuruluşları, kamu kurumlarına yol gösterici nitelikte bir ulusal politika ve stratejinin geliştirilmesi gerekmektedir

2. Yasal çerçevenin oluşturulması: Cana veya mala etki eden siber saldırı veya tehditlerin suç olarak tanımlanması ve cezalandırılması, özellikle siber saldırganların caydırılması konusunda büyük önem teşkil etmektedir.

3. Teknik tedbirlerin geliştirilmesi: Kamu kurum ve kuruluşların sahip oldukları bilgi ve iletişim teknolojilerinin yazılım ve donanım parçalarının da güvenliğinin sağlanması gerekmektedir.

4. Kurumsal yapılanmanın belirlenmesi: Asıl görevi siber güvenliği sağlamak olan kamu kurumunun görev ve sorumlulukları ile diğer kuruluşlar ile nasıl çalışacağı hususları yasal açıdan net olarak belirlenmelidir ve gerekli olan idari, mali ve teknik imkan ve kabiliyetler sağlanmalıdır.

5. Ulusal işbirliği ve koordinasyonun sağlanması: Güvenliğin sağlanabilmesi için ise tüm kurum ve kuruluşlar arası sıkı bir işbirliği ve koordinasyon sağlanmalıdır

6. Kapasitenin geliştirilmesi: Bilişim teknolojilerinde yaşanan gelişmeler, siber saldırı ve tehditlerin araç ve yöntemlerini de değiştirmiş ve geliştirmiştir. sistemlerin güvenliğini

sağlama konusunda uygulanacak politikalar, yasalar, standartlar, ürünler ve çözümler de bu değişim ve gelişime uygun olarak oluşturulmalıdır.

7. Farkındalık Oluşturma: İletişim araçları kullanılarak kişiler, değişen siber saldırı araç ve yöntemleri konusunda bilgilendirilmeli, farkındalık ve bilgi düzeyleri yükseltilmelidir.

8. Uluslararası işbirliği ve uyumun sağlanması: bireysel, kurumsal ve ulusal tüm altyapı ve sistemler internet üzerinden birbirlerine bağlıdır. Bu ağın güvenliği ise ancak uluslararası işbirliği ve koordinasyon ile sağlanabilir. Bu işbirliği çerçevesinde ortak bir mevzuatın oluşturulması, suç soruşturma ve kovuşturma usul ve yöntemlerinin uyumlu hale getirilerek, bilgi paylaşım mekanizmalarının oluşturulması gerekmektedir. (Canbay & Ünver, 2010)

Ülkemizce bahsi geçen hususlar ve gelişen, yeni ortaya çıkan tehditler doğrultusunda alınan siber güvenlik tedbirleri ve siber uzay konusunda yapılan çalımalar ışığında yapılan araştırmaların birleştirilmesi sonucunda ortaya çıkmış Ülkelerin Siber Güvenlik Güçleri sıralaması Tablo 3.4'te belirtilmiştir. ITU tarafından yayınlanan siber güç endekslerinin bulunduğu tablo ise aşağıdaki gibidir.

Sıra Nu.	Ülke	Siber Savunma	Siber Saldırı	Siber Uzaya Bağımlılık	Toplam Siber Güvenlik Güçleri	Siber Güvenlik Güçleri
1	ABD	9,5	8,95	1,1	19,55	**6,52**
2	Çin	7,27	7,5	4,4	19,17	**6,39**
3	Hindistan	5,99	3	6,5	15,49	**5,16**
4	Almanya	7,47	5,4	2,1	14,97	**4,99**
5	Fransa	7,43	4,17	3,2	14,8	**4,93**
6	İtalya	6,25	3,78	4,7	14,73	**4,91**
7	Rusya	6,88	4,66	2,95	14,49	**4,83**
8	Brezilya	5,73	3,46	5,2	14,39	**4,8**
9	Türkiye	5,26	2,32	5,85	13,43	**4,48**
10	Kuzey Kore	3,07	0,82	9,5	13,39	**4,46**
11	Japonya	7,04	5,79	0,45	13,28	**4,43**
12	Kanada	6,25	4,11	2,55	12,91	**4,3**
13	İsrail	7,11	2,87	2,85	12,83	**4,28**
14	İngiltere	7,6	4,59	0,5	12,69	**4,23**
15	Güney Kore	6,24	4,29	1,7	12,23	**4,08**
16	İran	2,94	0,82	7,05	10,81	**3,6**

Tablo 3.4. Ülkelerin siber güvenlik güçleri sıralaması (Çeliktaş, 2016)

Tablo 3.5. Türkiyenin küresel siber güvenlik göstergesi (Canbek, 2016)

Yukarıda yer alan iki tablodan ülkemizin siber güvenlik tedbirlerinde ortalama bir konumda olduğunu, Siber uzaya bağımlılığın ortalamanın üzerinde olduğu ve siber saldırı gücümüzün ise düşük olduğunu görebiliyoruz. Ülkemizce alınan güvenlik tedbirlerin savunma odaklı olması sebebiyle siber savunma gücümüz ortalamada iken, saldırı gücümüz düşük konumda yer almıştır. Bu farklığın temeli siber güvenlik kavramında da farklı yaklaşımların olmasıdır.

Siber güvenlik yaklaşımları

Bilgisayar ve iletişim sistemlerinin hızlı bir şekilde ilerleyerek İnsan hayatına etki eder noktaya geldiği günümüzde insanların sosyal hayat, alışveriş ve iletişim alışkanlıklarını önemli ölçüde değiştirmiş ve insan hayatı için vazgeçilmez noktaya gelmiştir.

Bilişim sistemleri ve teknolojinin toplumlarda yaygınlaşması ve insan hayatına önemli ölçüde sağladığı kolaylıklar ve kazanımlar nedeniyle insanları bu teknolojiyi daha fazla kullanmak zorunda bırakmıştır.

Küresel boyutta artan internet ve bilişim teknolojilerinin kullanımı siber güvenliğe yönelik yaklaşımlar ortaya çıkmıştır. Mulligan ve Schneider bu yaklaşımları aşağıdaki gibi açıklamıştır.[63]

Önleme/korunma yaklaşımı

Önleme/Korunma Yaklaşımın amacı sistem güvenliği için azami derecede dikkat edilmesi herhangi bir zafaa sebebiyet verilmemesidir. Zafiyetlerin olmayışı siber güvenlikte yaşanacak saldırı ihtimalini ortadan kaldıracak ve sistem güvenliği sağlanmış olacaktır.

Bu yaklaşımın en önemli eksiği insan faktörünün göz ardı edilmesidir. Yazılım kodlarının çok uzun, karmaşık ve kontrol edilmesinin zor oluşu hata olasılığını arttırmakta ve her hata hedeften sapmaya neden olmaktadır.

Risk yönetimi yaklaşımı

Risk Yönetimi Yaklaşımında siber güvenliğin her sistem için şart olmadığı mantığıyla hedef belirlenmemiştir. Siber güvenliğe yatırım yapıldığında amaca ulaşmak için zararlar en aza indirilmelidir. Yatırımların ve risk değerlendirmelerinin amacına uygun yapılıp yapılmadığı ve kaynakların doğru yönetilip yönetilmediği, ancak siber saldırılar olduğunda değerlendirilebilecektir. Siber güvenlik seviyesi ölçülebilir düzeyde değildir. Risklerin hesaplanmasında zararlar ve olası kayıplar hakkındaki bilgilerin hesaplanma zorluğu yaklaşımın eksik yönü olarak değerlendirilebilir. Siber güvenlikte tüm zafiyetler eşit değildir, dolayısıyla yalnızca algılanan ve sistem içerisinde büyük maddi hasara neden olabilecek tehditlere ulaşmaya odaklanılır.

Siber caydırıcılık yaklaşımı

Bilişim sistemlerine zarar verecek saldırıyı başlatan şahısları bu eylemi gerçekleştirmeden vazgeçirmek şeklinde tanımlanabilir.

Bilişim sistem ve altyapılarına yapılan Siber saldırıların suç kapsamında değerlendirilerek, faillerin tespiti, adli soruşturma ve cezalandırmalara önem verilmesini savunan bir yaklaşımdır. Kritik alt yapı sistemlerine zarar verecek Saldırganların yakalaması ve yargılanmasına yönelik çalışmalar yapılarak saldırıların engellenmesine çalışılır.

[63] Deirdre K. MulliganandFred B. Schneider, "DoctrineforCybersecurity", ***TheJournal of theAmerican Academy of Arts&Sciences***, Daedalus, Fall 2011, Vol.140, No.4, 70-92, pp.1-14, http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf,. (Erişim Tarihi: 25 Şubat 2015).

Kamu siber güvenliği yaklaşımı

Kamu yararına sunulan diğer hizmetler gibi siber güvenlik de geliştirilmeye çalışılmalı, kurumlarda siber güvenliği sağlamanın önemli bileşeni tüm çalışanların bilgi güvenliği farkındalığını en üst seviyeye çıkarmaktır. Siber güvenlikte risk durumları iyi analiz edilmeli ve güvensizlik durumları iyi yönetilmelidir. Bu yaklaşımda siber saldırıların engellenmesi ve etkilerinin asgari seviyeye indirilmesine çalışılmaktadır.

Kurum ve kuruluşların varlıklarının korunması konusunda bilgi güvenliğindeki gizlilik, bütünlük, erişebilirlik konularına dikkat edilmesi gerekmektedir. Sadece ilgili olan kişilerin görmesi, kullanması gizlilik, yapılacak herhangi bir siber saldırıda bilginin yetkisiz kişilerin eline geçmesi varlığın gizliliğinin de ihlali anlamına gelmektedir. Bilginin bütünlüğünün korunmasındaki amaç saklanan verinin yetkisiz kişiler tarafından değiştirilmesini veya bozulmasını önlemektir. Erişebilirlik bilgiye ihtiyaç duyulduğunda erişebilmektir[64]

Siber güvenlik stratejilerinde öne çıkan unsurlar ve Türkiye'deki siber güvenlik politikaları

Bilişim sistemlerinin yaygınlaşması ve küresel boyutta artan internet kullanımı sonucu siber güvenlik ulusal güvenlik stratejilerinde yer almaya başlamıştır. Başta gelişmiş ülkeler olmak üzere pek çok ülke ve NATO, AB gibi uluslararası kuruluşlar siber güvenlik stratejileri üretmiştir. 19 ülkenin ulusal siber güvenlik stratejileri üzerinde yapılan inceleme sonucunda strateji belgelerinde şu ortak hedeflere değinildiği görülmektedir (Luiijf ve diğ.'den aktaran Klimburg, 2012: 56):

• Güvenli, saldırılara karşı dayanıklı ve güvenilir bir siber alanın sağlanması.

• [Bilişim sistemleri vasıtasıyla] ekonomik ve sosyal refahın, güvenli iş ortamı ve ekonomik büyümenin teşvik edilmesi.

• Bilişim ve iletişim teknolojilerinin barındırdığı risklerin kontrol altında tutulması.

• Bilişim altyapılarının dirençli hale getirilmesi.

Siber alanda stratejik değişim algısına yönelik olarak ülkelerin siber savaş stratejilerinin etkileyeceği hususlar Çifçi'ye (2012:66) göre şu şekildedir:

- Siber alana doğrudan veya dolaylı olarak uygulanabilecek olan ulusal, uluslararası yasal düzenlemeler ve ülkeler arası sözleşmeler,
- Ülkenin rejimi, insan hakları ve demokrasiye olan yaklaşımı,

[64] http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php

- Ülkenin uluslararası camiada kendini konumlandırmak istediği yer ve bu kapsamda mücadelesini hangi alanlara taşıyacağı,
- Ülkenin siber alanı kullanma yaygınlığı ve siber alana olan bağımlılığı,
- Ülkenin siber savunma ve saldırı kabiliyetleri.

Klimburg (2012) ulusal siber güvenliği düşünülürken göz önünde bulundurulması gereken beş alan olduğunu belirtmektedir. Mevcut siber güvenlik stratejilerine bakıldığında bu alanların işlendiği görülmektedir.

1- Askeri siber operasyonlar (denilince öncelikle akla gelen ülkenin sahip olduğu bilişim altyapısının korunmasına yönelik olarak siber savunma olmaktadır.)

2- Siber suçlarla mücadele edilmesi konusudur

3- İstihbarat/karşı istihbarat faaliyetleri konusu

4- Siber güvenlik kriz yönetimi ve kritik altyapıların korunmasıdır.

5- Siber diplomasi ve internetin yönetimidir.

Türkiyenin siber güvenlik uygulamaları

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Türkiye'nin ilk siber güvenlik strateji belgesidir. 2012 yılına kadar Bilim, Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde BTK tarafından sivil toplum kuruluşları ve kurumları ile beraber yürütülen siber suçlarla mücadele, Aralık 2012'de "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının" hazırlanarak yürürlüğe girmesiyle Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumluluğuna verilmiştir. 2013-2014 eylem planında, gerekli mevzuat çalışmalarının yapılması, siber güvenlikle ile ilgili tatbikatların yapılması, siber güvenlikle ilgili eğitim ve farkındalık arttırılmasına yönelik çalışmalar yapılması konularında eylemelere yer verilmiştir.[65]

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar gereğince; Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır[66].

[65] Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" www.resmigazete.gov.tr, Haziran 2013
[66] https://www.btk.gov.tr/siber-guvenlik-kurulu

Siber Güvenlik Kurulana yüklenen görevler aşağıdaki gibidir.

• Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak,

• Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak,

• Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek,

• Kanunlarla verilen diğer görevleri yapmak.

Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında toplanan Siber Güvenlik Kurulu aşağıda belirtilen kurumlardan ve üst düzey yöneticilerden oluşmaktadır

• Dışişleri Bakanlığı Müsteşarı,

• İçişleri Bakanlığı Müsteşarı,

• Milli Savunma Bakanlığı Müsteşarı,

• Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,

• Kamu Düzeni ve Güvenliği Müsteşarı,

• Milli İstihbarat Teşkilatı Müsteşarı,

• Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,

• Bilgi Teknolojileri ve İletişim Kurumu Başkanı,

• Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı,

• Mali Suçları Araştırma Kurulu Başkanı,

• Telekomünikasyon İletişim Başkanı

Ulusal Siber Güvenlik Stratejisine göre güvenlik anlamında orta ve uzun vadede öncelikle dikkat edilmesi gereken bazı konular ve atılması gereken adımlar aşağıda belirtilmiştir. (Alkan M. , Sağıroğlu,Ş. , Canbek, G. , Ünver, M. , Yazıcı, A., 2012)

1-Yasal Düzenlemeler: Uluslararası hukuk kuralları, kamu yararı, kritik altyapı sistemlerinin korunması ve kişisel veri güvenliğinin sağlanması amacıyla siber suçlarla mücadele kapsamında yasal düzenlemeler yapılıp uygulanmalıdır.

2-Kurumsal yapılanma: Kurumsal yapılanmaların oluşturulması, strateji belirleme kurumu, Ulusal siber güvenlik merkezi, müdahale merkezi gibi yapılar faaliyete geçirilerek devlet kurumları ve sivil oluşumlar arasında koordinasyon sağlanmalıdır.

3-Eğitim: Bireylerin siber güvenlik konusunda eğitilmesi, lisans lisansüstü eğitim programları açılarak eğitimde farkındalık oluşturulmalı.

4-Siber Güvenlik Kültürünün Oluşturulması: Kamu kurum ve kuruluşları personelleri siber güvenlik konusunda eğitilmeli ve bilinçlendirilmelidir.

5-Kamu, Üniversite ve Özel Sektör İşbirliği: Akademik programların yaygınlaştırılması kamu-üniversite-özel sektör arasında işbirliği sağlanmalıdır.

6-Milli Teknoloji Geliştirme: Siber güvenlik alanında yazılım ve donanımların yerli ve uluslararası standartlara uygun olarak üretilmesi ve yerli ürünlerin kullanımı yaygınlaştırılmalıdır.

7-Uluslararası İşbirliği: Uluslararası aktivitelere katılmak. BM, AB, OECD gibi kuruluşlar bünyesinde çalışmalara destek verip katılmak, bölgesel anlaşmalara taraf olmak.

8-Belgelendirme: Kamu kurumlarının belgelendirme konusunda eksikleri giderilmeli ve uluslararası güvenlik sertifikaları ile belgelendirilmesine önem verilmeli.

Türkiye'nin 2013-2014 siber güvenlik eylem planında gerçekleştirilmesi hedeflenen adımlar aşağıda belirtilmiştir. [67]

- Siber Güvenlik Konusunda Yasal düzenlemelerin Yapılması
- Siber Olayların Delillendirilmesi ve ileri teknoloji ürünlerinin temini sağlanması
- Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması
- Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı ve risk analizlerinin yapılması
- Kamu Bilgi Güvenliği Programı Yürütülmesi
- Siber Güvenlik Eğitim Altyapısının Güçlendirilmesi ve yaygınlaştırıması.
- Siber Güvenlik Tatbikatlarının Düzenlenmesi ve Çalıştaylara önem verilmesi.
- Kamu Güvenli İletişim Kurallarının Belirlenmesi

[67] Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" www.resmigazete.gov.tr, Haziran 2013

- Yazılım Güvenliği Programının Yürütülmesi
- Siber Tehditleri Önleme Projesinin Yürütülmesi
- Siber Güvenlik Konusunda Ürünlerin ve Hizmet Sağlayıcıların Belgelendirilmesi
- Adli Bilişim Konusunda Hizmet Sağlayıcılara Güvenlik Belgesi Verilmesine Yönelik Kuralların Belirlenmesi
- İş Sürekliliği ve Veri Yedekleme Sistemleri Kurulması
- Kamu Kurum ve Kuruluşlarının İnternet Sayfalarının Yerli Veri Merkezlerine Taşınması
- Veri Sızmasını Tespite Yönelik Test Altyapısı Geliştirmesi ve Uygulamaya Alınması
- Kamu Kurumlarında Verilere Erişim Düzeylerinin Belirlenmesi
- Açık Kaynak Kodlu Ürünlerin Kullanımının Teşvik Edilmesi
- Siber Güvenlik Konusunda Akademisyen Yetiştirilmesi
- Siber Güvenlik Uzmanlığına Yönlendirme Programları ve sertifikasyon çalışmalarının Yürütülmesi.
- Bilgisayar Kullanıcılarının Siber Güvenlik Konusunda Bilinçlendirilmesi
- Ulusal ve Uluslararası Siber Güvenlik Etkinlikleri Düzenlenmesi
- Ar-Ge Çalışmalarının Teşvik Edilmesi.
- Siber güvenlikte teknolojinin millileştirilmesi ile daha güvenli donanım ve yazılımların kullanılmaya başlanması.
- Ulusal Siber Güvenliğin Milli Güvenliğe Entegrasyonu

2016 yılı itibariyle, ikinci strateji belgesi 2016-2019 dönemi için hazırlanmış ve yürürlüğe girmiştir. Türkiye'nin siber güvenlik konusunda izleyeceği yolu belirleyen 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kamu ve özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ek olarak, sanayi, özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın bütün bileşenlerini kapsamaktadır. Strateji hazırlıkları geniş katılım sağlanarak gerçekleştirilmiştir[68]

[68] T.C. UDHB , 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, T.C. UDHB Yay. Ankara, 2016.

Ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak ilkeler aşağıdaki gibidir.[69]

1. Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.

2. Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir.

3. Risk yönetimi, teknik zaafların hızla giderilmesini, saldırı ve tehditlerin önlenmesini, fark edilmesini, yanıtlanmasını ve muhtemel zararın en aza indirgenmesini içerir.

4. Siber uzay güvenliğinin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir.

5. Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir.

6. Paydaşlar siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurur.

7. Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır.

8. Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.

Bu stratejik eylem kapsamında devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek riskleri azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır.

2016-2019 döneminde, mevcut riskleri, belirlenen ilkeler ışığında asgari düzeye indirmeyi hedefleyen stratejik amaçlar aşağıdaki gibidir. (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016: 13,14):

[69] T.C. UDHB , 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, T.C. UDHB Yay. Ankara, 2016.

1. Kritik altyapı sektörlerin envanterinin oluşturulması, güvenlik ihtiyaçlarının karşılanması ve güvenlik denetlemelerinin düzenli olarak yapılması,

2. Uluslararası standartlara uygun bir şekilde siber güvenlik mevzuatının oluşturulması,

3. Sektör düzenleyici kurum ve kuruluşların siber güvenlik düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi,

4. Kritik altyapı sektörlerinin sadece saldırganlardan değil, aynı zamanda kullanıcı hataları ve doğal afetlerden de korunması için düzenlemelerin yapılması,

5. Her kurum kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ve kapasiteye erişmesi,

6. Siber güvenlik konusunda kurum ve kuruluşların yöneticilerin farkındalık seviyelerinin artırılması,

7. Siber güvenlik alanında personel yetiştirilmesi ve bu alanda çalışmak isteyen personel, öğrenci ve araştırmacıların teşvik edilmesi,

8. Toplumun her kesimi ve seviyesinde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilaveten yazılı ve görsel medyada farkındalık çalışmalarının yapılması,

9. Kamu kurumlarında siber güvenlik uzmanı istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi,

10. Kurumsal ve Sektörel SOME'lerin etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve bilgi paylaşımının geliştirilmesi,

11. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması,

12. Kamu kurumları, özel sektör, STK'lar, denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyonu ile ulusal siber güvenlik eko-sisteminin oluşturulması,

13. Ulusal Siber güvenlik eko-sistemi içinde danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması,

14. Kritik altyapıların kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin açıklıkların kötüye kullanılmasına engel olmak amacıyla sertifikasyon çalışmaları ve açıklık analizlerinin yapılması,

15. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması,

16. Siber güvenlikte dışa bağımlılığı azaltmak için AR-GE faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi,

17. Tehdit unsurlarının saldırı yapmadan önce de bertaraf edilememesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi,

18. Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 teknolojilerinin yaygınlaştırılması.

2016-2019 döneminde gerçekleştirilmesi planlanan stratejik eylemler aşağıdaki başlıklar altında toplanmıştır:

1-Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması

2-Siber Suçlarla Mücadele

3-Farkındalık ve İnsan Kaynağı Geliştirme

4-Siber Güvenlik Ekosisteminin Geliştirilmesi

5-Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Siber savunmanın güçlendirilmesi ve kritik altyapıların korunması

Stratejik eylem ile hedeflenen, devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek riskleri azaltmaya yönelik faaliyetlerin planlanmasıdır.

Siber suçlarla mücadele

Stratejik eylem ile hedeflenen kurumları ve bireyleri etkileyen, ağırlıklı olarak maddi kayba yol açan riskleri azaltmaya yönelik faaliyetlerin planlanmasıdır.

Farkındalık ve insan kaynağı geliştirme

Stratejik eylem ile hedeflenen kurum yöneticilerinden bilgisayar kullanıcısı vatandaşa kadar toplumun tüm kesimlerine siber güvenlik kültürünün kazandırılmasına yönelik eylemlerin gerçekleştirilmesi ve siber güvenlik uzmanı yetiştirilmesi planlanmaktadır.

Siber güvenlik ekosisteminin geliştirilmesi

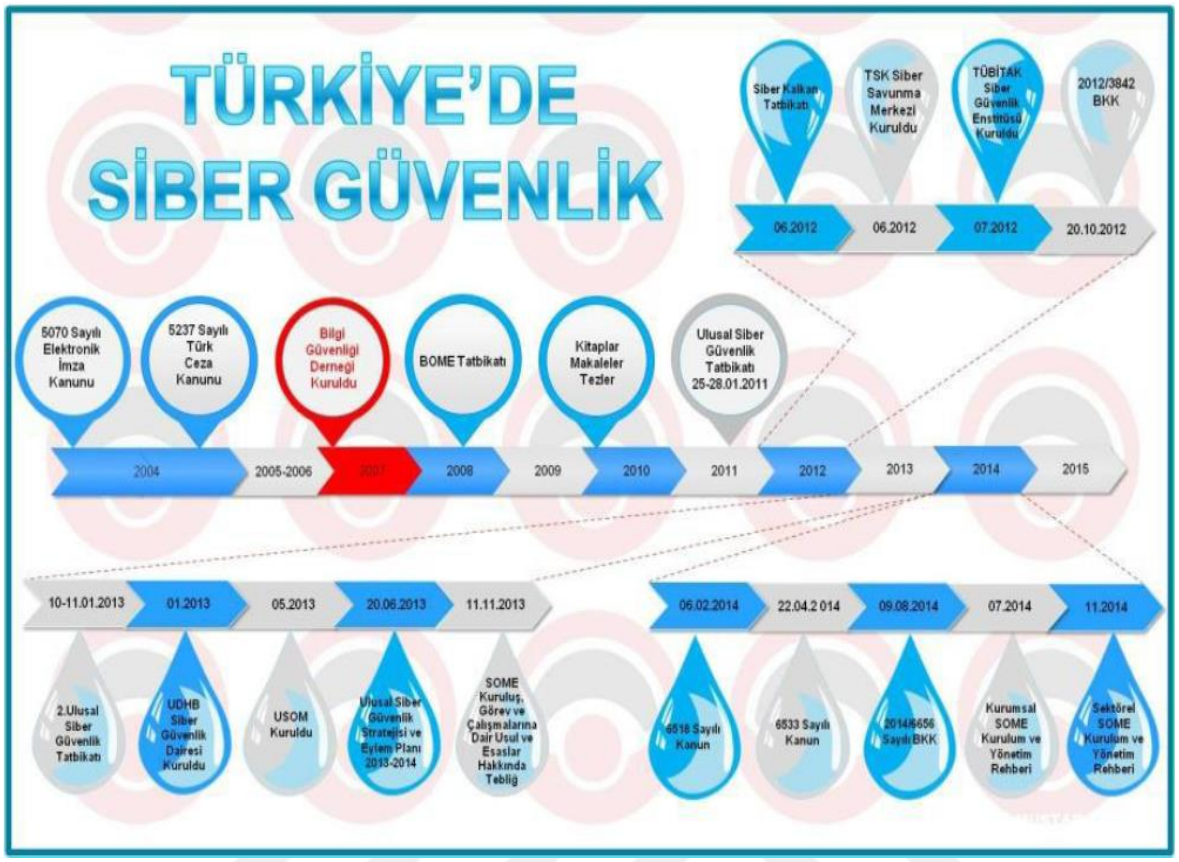
Stratejik eylem ile hedeflenen kamu, özel sektör, STK ve diğer paydaşların koordineli katkısıyla mevzuattan teknolojiye kadar gereksinimlerin belirlenmesine ve uygulamaya dökülmesine yönelik eylemlerin gerçekleştirilmesi planlanmaktadır.

Siber güvenliğin milli güvenliğe entegrasyonu

Stratejik eylem ile hedeflenen devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek, iyi organize olmuş tehdit unsurları tarafından gerçekleştirilecek kasıtlı saldırıların verebileceği zararı azaltmaya dönük eylemlerin gerçekleştirilmesi planlanmaktadır.

2016-2019 Ulusal Siber Güvenlik Stratejisinin son başlığı olan milli güvenliğe bütünleşme konusu siber tehditlerin artık ulusal boyuta ulaştığının ve devlet politikası olarak bu konunun ele alınmasının, çalışmanın savunduğu şekilde siber güvenliğin milli güvenlik için yadsınamaz öneme sahip olduğunun en bariz göstergesi olmuştur.

Ülke olarak siber güvenlik alanında planlı bir süreç işletilerek siber güvenlik tedbirleri en üst seviyede alınmıştır. Güvenlik alanındaki temel faaliyetlerin kısa özeti mahiyetindeki aşağıda yer alan tablo teknolojik genişlemeye paralel olarak siber güvenlik tedbirlerimizin de arttığını göstermektedir.



Şekil 3.5. Türkiyede siber güvenliğin gelişimi (Ünver, 2015)

Ülkemizce alınan tedbirlere örnek olması ve bazı örnek uygulamaların sonuç kısmında tavsiye edilen uygulamalar arasında olacak olması sebebiyle dünya üzerinde yer alan uygulama örneklerinin incelenmesi çalıma için bir gereklilik ve siber güvenliğin milli güvenlik açısından önemini gösterir nitelikte olacaktır.

Dünyadaki siber güvenlik uygulamalarına örnekler

1) ABD

Siber suçlarla mücadele kapsamında 1996 yılında ABD Başkanına bağlı "Commission of Critical Infrastructure Protection" adlı bir komisyon kuruldu.[70] Bu komisyon internet alanında çalışma yapan ilk ulusal komisyon olarak kabul edilmektedir. ABD'de siber suçları önlemek amacıyla FBI kurumuna bağlı "National Infrastructure Protection Center" ve "Computer Crime Squad" adlarıyla iki merkez kurulmuştur. (Atıcı & Gümüş, 2003)

ABD siber savunma konusunda dünyada önde gelen ülkelerden biridir.2001 yılındaki olaylardan sonra siber güvenlik devlet politikası olarak benimsenmiş ve Ulusal siber

[70] https://www.hsdl.org/?abstract&did=487492 Erişim Tarihi: 19/11/2019

güvenlik politikasını 2003 yılında yayınlamıştır. Beyazsaray'da bulunan ABD başkanına bağlı ulusal siber güvenlik çalışmalarını yürüten Siber Güvenlik Ofisi Siber saldırılar karşısında Federal birimler arasında koordinasyonu sağlamakla görevlidir.

2011 tarihli ABD Savunma Bakanlığının Siber Uzayda Harekât Stratejisi(Department of Defence Strategy for Operating in Cyberspace) belgesi aşağıdadır;[71]

- ABD Savunma Bakanlığı'nın siber uzayın tüm imkânlarından faydalanabilecek şekilde organize edilmesi, eğitimi ve donanımı için tüm siber uzayın harekât alanı olarak kullanılması,
- ABD Savunma Bakanlığı ağ ve sistemlerinin korunması için yeni savunma konseptlerinin uygulanması,
- Devletin hep beraber siber güvenlik stratejisinin etkinleştirilmesi için, ABD'deki diğer bakanlıklar, kamu kurumları ve özel sektör ile ortak çalışmalar yapılması,
- Siber güvenliğin güçlendirilmesi için ABD'nin müttefikleri ve uluslararası ortakları ile güçlü ilişkiler kurulması,
- Yetenekli siber işgücü ve hızlı bir şekilde elde edilecek teknolojik yenilikler vasıtasıyla milli yeteneklerin geliştirilmesi

ABD'deki siber güvenlik gelişmelerinin önemli olanlarını sıralayacak olursak bunlar: 2002 yılında National Strategy to Secure Cyberspace (Siber Alanın Güvenliği için Ulusal Strateji), 2006 yılında National Infrastructure Protection Plan (Ulusal Altyapı Koruma Planı), 2007 yılında National Strategy for Information Sharing (Bilgi Paylaşımı Ulusal Stratejisi), 2008 yılında Comprehensive National Cybersecurity Initiative (Kapsamlı Ulusal Siber Güvenlik İnisiyatifi - CNCI) ve 2009 yılında Obama tarafından siber güvenlik koordinatörü atanmasıdır.

ABD'nin, siber güvenliğin sağlanması, politika ve stratejilerini gerçekleştirmek için görevlendirdiği en üst düzeyde dört kurum bulunmaktadır. (Çifçi, 2013)

1. Siber Komutanlık (U.S.Cyber Command - USCYBERCOM)

2. Milli Güvenlik Teşkilatı (National Security Agency - NSA)

3. Federal Araştırma Bürosu (Federal Bureau of Investigation - FBI)

[71] Department of Defense Strategy for Operatıng in Cyberspace, Department of Defense, USA, 2011, s.5-10.

4. İç Güvenlik Bakanlığı (Department of Homeland Security - DHS)

2) ÇİN

Çin Halk Cumhuriyeti siber savunmaya büyük önem vermiştir. Çin de siber güvenlik faaliyetleri Çin Ordusu tarafından yürütülmektedir. Bu amaca hizmet etmek için Çin Halk Kurtuluş Ordusu'nun (People's Liberation Army – PLA) üzerine büyük bir destek vermiştir ve siber güvenlikten birinci dereceden sorumlu olarak orduyu tutmuştur Ordu bünyesinde siber saldırı ve savunma konularına çalışan uzmanlardan oluşan iki ayrı grup bulunmakta ve sadece siber güvenlik üzerine faaliyet gösteren ARGE yapısı bulunmaktadır.

Ayrıca 'Altın Kalkan'[72] adı verilen güvenlik duvarınasahip olan ülkenin siber saldırılara karşı güçlü olduğu bilinmektedir.[73]

3) İNGİLTERE

İngiltere siber savunmaya bütçesinde büyük pay ayırmış ve siber tehditleri ülke güvenliğini riske atan birinci öncelikli tehdit olarak görmüştür. İngiltere hükümeti 2010 yılında yayınladığı siber Güvenlik raporu ve 2011 yılında yürürlüğe koyduğu Ulusal Siber Güvenlik Stratejisi ile önemli adımlar atmıştır.

İngiltere'nin siber güvenlik için ortaya koymuş olduğu hedefler şunlardır[74]

(1) Siber suçlar ile mücadele etmek ve siber alanda iş yapılabilecek dünyada en güvenli yer olmak,

(2) Siber saldırılara dayanıklı olmak ve siber alanda çıkarlarını iyi savunmak,

(3) Halkının güvenli olarak kullanabileceği ve açık toplumu destekleyen açık, kararlı ve canlı bir siber alanın oluşumuna katkıda bulunmak,

(4) Hedeflere ulaşabilmek için gereken her tür bilgi, yetenek ve kapasiteye sahip olmak.

[72] https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf
[73]https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html
[74] UK Cabinet Office. "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World", Cabinet Office, <http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategyfinal.pdf>, 17.05.2012.

4) RUSYA

Rusya, "Savaşın Yeni Alanı" olarak gördüğü siber uzayda askeri AR-GE çalışmalarına önem vermiştir. Siber uzaydan gelecek tehditlere karşı Rusya Silahlı Kuvvetleri içerisinde siber birliklerin kurulması kararlaştırılmıştır.[75]

2000 yılında Putin tarafından siber tehditler ile mücadele etme konusunda yasal altyapıyı oluşturacak "Rusya Bilgi Güvenliği Doktrini" kabul edilmiştir. Rusya için siber güvenlik alanında atılan en önemli adım 2009 yılında Shangai Cooperation Organization ile bilgi güvenliği konusunda imzalamış olduğu anlaşmadır. Anlaşmanın hedefi imza eden taraflar ve ilgili ulusal ajanslar arasında güveni ve işbirliğini artırmak maksadıyla politik ve yasal müesseseler kurmaktır.

Rusya'da siber güvenlikten sorumlu olan organizasyonlar;

- Güvenlik Konseyi,
- Federal Güvenlik Hizmetleri (FSB),
- Federal Savunma Hizmetleri,
- Federal Teknik ve İhracat Hizmetleri ve
- Bilgi Teknolojileri ve İletişim Bakanlığı şeklindedir.

[75] European Parliamentary Research Service (2014), Cyber defence in the EU Preparing for Cyber Warfare?, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143Cyber-defence-in-the-EU-FINAL.pdf (15.03.2016). 2014:5

4. SONUÇ

Bilgi ve iletişim teknolojilerinin hızla gelişimi ve günümüzde ulaştığı nokta, başta internet olmak üzere bütün siber uzay elemanlarının hayatımızın vazgeçilmez bir unsuru haline gelmesini sağlamış ve artan bu bağımlılık bütün hayatımızı etkisi altına alması sebebiyle güvenlik kaygılarını da beraber getirmiştir. 5. Boyutu hayatımıza sokan bilişim alanındaki gelişim süreci duraksamadan ilerlemeye devam etmektedir. Bu gelişme süreci çok boyutlu güvenlik anlayışının benimsenerek ulusal güvenlik stratejilerinde ve uluslararası ilişkilerde siber uzay boyutunun göz ardı edilmemesi gerekliliğini doğurmuştur.

Siber uzayın genişlemesi ve genişlemesine temel rolü oynayan internet, gelişimin ve teknolojinin ana unsuru olan bilgiye ulaşım ve paylaşımı kolaylaştırmıştır. Türkiye'de araştırma yürüten bir bilim insanının dünyanın öteki ucunda yer alan diğer bilim insanından anında yardım alabilmesi internetin hayatımıza kattığı iletişim ağı sayesinde gerçekleşebilmektedir. Tıpkı geçmiş zamanlardaki iletişim ve ulaşım ağlarının güvenliğinin sağlanması gibi internet iletişiminin gizlilik, bütünlük ve erişilebilirliğinin sağlanması ulusal boyutunda dışında uluslararası bir gereklilik haline gelmiştir. Fakat günümüzde siber uzay için uluslararası boyutta bir bütüncül yaklaşım sağlanamamıştır. Buna rağmen ülkeler kendi ulusal güvenlikleri için milli güç unsurlarının içerisine siber güvenlik alanını da dâhil etmektedirler.

Bu bağlamda, güvenlik ve uluslararası güvenlik kavramları klasik yapısından farklı bir yapıya bürünerek sanal dünyaya yönelmiştir. Bu sebeple farklı boyut olan siber uzayda yer alan siber silahlar da konvansiyonel silahlar gibi savaş alanında ve uluslararası ilişkilerde yeni aktör olarak yer almaya başlamışlardır. Bu yeni aktörü de politika üretirken göz ardı etmemek gerektiği kadar bu aktörün ortaya çıkarabileceği sorunlara karşı tedbirli olunmalıdır. Siber saldırıların güvenlik politikaları hatta milli güvenlik politikaları içerisinde kritik nokta olarak ele alınmasının caydırıcılığının dünyada yaşanan örneklerinde de görüldüğü şekliyle üst seviyede olmasıdır.

Bireyselliğin ötesine geçerek dünya geneline yayılan bu tehditlerin tamamen ortadan kaldırılması siber uzayın sağladığı anonimlik sayesinde ve günümüz şartlarında zor olsa da minimize edilebilir ve bunun için en temel şart ise devletlerin ortak bir siber uzay hukukunu, etiğini kabul ve bu konuda işbirliği yapmalarıdır. Fakat tıpkı terör konusunda bile ortak bir fikir birliği oluşturamayan dünya devletleri siber uzayda suç ve suçlulara yönelik ortak hareket veya siber terör konusunda ortak akıl ortaya koyamamıştır. Fakat ortak bir kabul

olmasa dahi ülkeler arasında işbirliği, bilgi paylaşımı, eğitim, destek, ortak soruşturma yürütme vb. konularda ortak faaliyetler yürütülmektedir.

Devletler ise milli bir güvenlik sorunu olan siber güvenlik konusunda kendi güvenliklerini almak yönünde adımlarını atmalıdırlar ve ülkemiz örneğinde olduğu gibi ülkeler için hayati öneme sahip kritik altyapı sektörleri başta olmak üzere devletin bütün kurumları için güvenliği tedbirler almalıdırlar. Kritik altyapı sektörlerine yapılacak bir siber saldırı neticesinde, nükleer santrallerde radyasyon sızıntısına, barajlarda su kapaklarının açılmasına, su dağıtım şebekelerine müdahale ile kirli suyun hatta karıştırılmasına, bankacılık ve finans sektörünün işlemez hale gelmesine, iletişim ağının devre dışı bırakılabilmesine, sebep olabildiği veya daha fazlasına sebep olabileceği düşünüldüğünde, siber güvenliğin milli güvenlik için ne denli kritik olduğu anlaşılacaktır.

Bu kritik güvenlik alanına karşı alınacak tedbirlerde, temel amacı bilgiye erişim ve bilgi paylaşımı olan internette erişim hakkı ile güvenliğin sağlanması arasındaki dengenin iyi kurulması, ulusal ve uluslararası mevzuatlara uygun hukuki altyapının sağlanması ve siber uzayın değişimine göre güncel tutulması, saldırıların asimetrik olması sebebiyle kaynağın belirlenmesindeki zorluklar için uluslararası işbirliği kurulması gereklidir. Ulusal düzeyde ise siber saldırılara karşı bu alanda faaliyet gösteren bilişim ve telekomünikasyon kurumları-şirketleri, servis sağlayıcıları, kolluk güçleri vb. kurum ve kuruluşların işbirliği ve koordinasyon içerisinde olmasının sağlanması gereklidir. Aynı zamanda siber güvenlik konferansları, bilgi paylaşım toplantıları, çalıştaylar kurumlar arasında işbirliği ve ortak akıl oluşturmak ve muhtemel bir saldırıya karşı hızlı reaksiyon vermek için gereklidir.

Çalışmada yer alan siber silahların türlerinin sürekli değiştiği ve geliştiği, siber saldırı türlerinin buna paralel olarak arttığı, örgütlerin ve devletlerin de dâhil olduğu siber terör eylemleri ve siber savaşların çıktığını bu beşinci boyutun getirdiği tehditlere karşı milli güvenliğimiz için alınan tedbirlere ek olarak alınacak güvenlik tedbirlerini milli teknik altyapı, hukuki zemin-işbirliği ve eğitim ve başlıklarında toplayabiliriz.

Bilişim alanında kullanılan yazılım ve donanımların büyük çoğunluğunun yurtdışı menşeli olması milli siber güvenlik için açık bir kapıdır. Yurtdışı menşeli yazılım veya donanımların içerisinde yerleştirilecek bir zararlı yazılım veya arkakapı (backdoor) milli siber güvenliğimizi müdahaleye açık hale getirecektir. Bu konunun yaşanmış bir örneği olmaması sürekli değişen uluslararası topludurumda olmayacağını garanti etmeyeceği için başta milli işletim sitemi olmak üzere her alanda milli yazılım ve donanım kullanımına başlanılmalıdır.

Kamu kurumları ve kurumsal şirketler ağ güvenliğini sağlamak için yerel ağlarını oluşturmaktadır. İnternet ağının dışında kendi milli ağımızın olması olası bir siber saldırıda internetin devre dışı kalması haline ortaya çıkacak olan iletişim kopukluğunu ortadan kaldıracaktır. İletişim ağının güvenliği sağlanmalı ve buna benzer çoğaltılabilecek örneklere karşı siber alanda faaliyet gösteren ticari kuruluşlar, resmi devlet kurumları ve üniversitelerce AR-GE çalışması yapılıdır.

Bu konuda yapılan ARGE çalışmalarının öncülüğünü TUBİTAK yapmaktadır. Milli işletim sistemi, milli yazılım üretiminin öncülüğünü yapan TUBİTAK tarafından geliştirilen yerli bir işletim sistemimiz olmasına rağmen, PARDUS adlı bu sistem hala hak ettiği bilinirliğe ve kullanıma ulaşabilmiş değildir. Çözüm yerli ürünlerin ortaya çıkarılması kadar bu ürünlerin pazarda yer alması veya alabilmesidir. Bu konuda öncülüğü kamu kurumları yapmalıdır. Kamu kurumlarında sistem kaynaklı bir siber saldırının geri dönüşü veya açtığı zarar tahmin edilemeyecek boyutta olabilir.

Dünyayı küresel köy haline getiren günümüz siber teknolojileri sebebiyle meydana gelen siber saldırıların tamamına yakına yurtdışı kaynaklıdır. Siber uzayın getirdiği anonimlik ve sınırları kaldırması sayesinde saldırılar küresel boyutta olmakta ve saldırıyı gerçekleştirenin tespitinde devletlerarası işbirliğini gerektirmektedir. Bu da bu alandaki güvenlik hizmetlerinin uluslararası yaklaşımlarla yürütülmesini gerekli kılmaktadır.

Bu sebeple siber güvenlik alanında diğer devletlerle işbirliği kurulmalı, hatta devletlerarası işbirliği ile siber suçlara veya siber savaşlara karşı ortak tavır alınmalıdır. Fakat mevcut durumda yaşanmış siber savaşların arkasında devletlerin resmi olarak olmasa bile bulunması, siber gücün devletler tarafından yaptırım aracı olarak kullanılması gerekçeleri ile bu işbirliğinin basit örnekleri olmakla birlikte geniş bir çevrede kurulması ve efektif olarak faaliyet göstermesi imkânsızdır.

Ulusal düzeyde ise yasal düzenlemeler siber dünyadaki gelişmelerin hızı karşısında geride kalmaktadır. Bu nedenle yasal mevzuat açıkları bir an önce kapatılmalı ve ihtiyaçlar doğrultusunda ve gelişmelerin paralelinde sürekli güncellenmelidir. Bunun yanı sıra yasa koyucular, meydana gelebilecek saldırıda delil olacak verilerin saklanmasını ve bunlara erişim konusunu netliğe kavuşturarak kamu ve şirketlerin maddi endişelerinin bireysel veri güvenliği ve suç ve suçlu ile mücadelenin daha önemli olması sebebiyle dikkate almamalıdır ve veri güvenliğini tesis etmelidir.

Üretilecek milli sistemlerin kullanılabilmesi, kullanıcı kaynaklı siber saldırılara karşı güvenliğin alınabilmesi, siber uzayın en zayıf halkası olan insan unsurundan kaynaklı hataları ve aksamaların en aza indirgenebilmesinin yegâne çözüm yolu ise eğitim ve bilinçlendirmedir. İnternete erişimin bu denli kolay olduğu, internet kullanım oranının % 80'lere yaklaştığı ve ilk kullanım yaşının giderek küçük yaşlara indiği günümüz Türkiye'sinde yürütülecek eğitim ve bilinçlendirme faaliyetleri ilkokul seviyesinden başlamalıdır. Okullarda bu konuda verilecek eğitimler ile başlayacak bilinçlendirme faaliyetleri toplumda ve kurumlarda verilecek konferans, eğitim vb. faaliyetlerle desteklenmelidir.

Ayrıca bilişim sitemlerinde çalışan personel düzenli olarak yenileme faaliyetine tabi tutulmalı ve siber uzayda meydana gelmiş değişikliklere karşı (yeni tehditler, sistem açıkları vs.) bilgilendirilmelidir. Ayrıca alınan bu tedbirler düzenli aralıklarla yapılacak tatbikatlarla test edilmeli ve siber güvenlik tedbirlerinin teoride kalmasının önüne geçilmelidir.

Özetle sanal âlem olarak dilimize yerleşmiş siber uzayın geleceğimizi şekillendirdiği ve buna devam edeceği, bu gelişim sürecinin güvenlik açıklarının sürekli olacağı ve bunlara tedbir alınmaması halinde bir savaştan daha şiddetli zararlara sebep olabileceğinin bilinerek güvenlik politikalarının şekillendirilmesi ve milli güvenliğimiz için zayıf nokta olmaktan çıkarılarak politik ve askeri güç olarak kullanabilecek seviyeye gelmemiz gerekmektedir. Bu hedefin sağlanmasında teknik donanımla alınan hiçbir siber güvenlik tedbiri bilinçli kullanıcının yerinin alamayacağı unutulmamalıdır.

KAYNAKLAR

A.Clarke, R., & Knarke, R. K. (2011). *Siber Savaş* (Cyber War) (çeviren:Murat Erduran). İstanbul Kültür Üniversitesi.

Ada, M. (2018). A*to Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi* . Gazi Üniversitesi Yüksek Lisans Tezi.

Alexander W. (1992). "Anarchy is What States Make Of It: The Social Construction Of Power Politics", *International Organization*, 46(2), 392.

Alkan, A. (2006). *21. Yüzyılın İlk Çeyreğinde Karadeniz Güvenliği.* Ankara: Nobel Yayın Dağıtım.

Arı, T. (2006). *Uluslararası İlişkiler Teorileri.* İstanbul: Alfa Yayınevi.

Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi,* 23(1), 238-244.

Atıcı, B., & Gümüş, Ç. (2003). Sanal Ortamda Gerçek Tehditler: Siber Terör. *Polis Dergisi*.

Avşar, Z. (2017). *İnternet Çağında Medya, Terör ve Güvenlik*. TRTAkademi, 116-132.

Aydın, M. (2013). *21. Yüzyılda Siber Güvenlik*. İstanbul: BİIgi Üniversitesi Yayınları.

Baitha, A. K., & Vinod, S. (2018). Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology*, 193-198.

Bakır, E. (2011). İnternet Güvenliğinin Tarihçesi. *TUBİTAK Bilgem Dergi*, 16.

Buzan, B. (1991). *People*, States and Fear. Londra.

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

Canbek, G., & Sağiroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 22(1).

Canbek, G. (2016). *Türkiyenin Küresel Siber Güvenlik Göstergesi*. HAVELSAN Aylık Siber Güvenlik Bülteni .

Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and cyberspace: Unique threat and response. *International Studies Perspectives*, 17(3), 307-321.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On Cyber Warfare*. Londra: Chatham House.

Çeliktaş, B. (2016). *Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme*. Trabzon.

Çırak, B., & Yörük, A. (2016). Mekatronik biliminin öncüsü İsmail El-Cezeri. *Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* (4), 175-194.

Çifçi, H. (2013). H. Çifçi içinde, *Her Yönüyle Siber Savaş*. İstanbul: TUBİTAK Popüler Bilim Kitapları.

Çıtak, Ö. (2016). *Ethical Hacking Offensive ve Defensive*. Level Kitap.

Çitlioğlu, E. (2008). *Gri Tehdit Terörizm*. Destek Yayınları.

Deirdre K. MulliganandFred B. (2011). Schneider, "DoctrineforCybersecurity", TheJournal of theAmerican Academy of Arts&Sciences, *Daedalus*, 140(4), 70-92.

Department of Defense Strategy for Operatıng in Cyberspace, Department of Defense, USA, 2011, 5-10.

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44(5), 643-666.

EGM (2011). *Kaçakçılık ve Organize Suçlarla Mücadele*. 2011 Raporu.

Elbahadır, H. (2012). *Hackıng Interface*. Kodlab.

Ercan, M. (2015). *Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri*. Gebze Teknik Üniversitesi Sosyal Bilimler Enstitüsü Strateji Bilimi Ana Bilim Dalı Yüksek Lisans Tezi. GEBZE.

Ertürk, F. E., & Yayan, G. (2012). Bilim ve Sanatı Birleştiren İki Usta. *Batman Üniversitesi Yaşam Bilimleri Dergisi*, 455.

Fan, W., Kevin, L., & Rong, R. (2017). Social engineering: Ie based model of human weakness for attack and defense investigations. *IJ Computer Network and Information Security*, 9(1), 1-11

Gençtürk, T. (2012). *Terör Kavramı Ve Uluslararası Terörizme Farklı Yaklaşımlar*. Başkent Üniversitesi Stratejik Araştırmalar Merkezi. Ankara.

Gündüz, M. Z. (2013). *Bilişim suçlarına yönelik IP tabanlı delil tespiti/IP-based evidence detection*.

Gündüz, M., & Daş, R. (2016). *Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri*. ISCTURKEY, (s. 11-18).

Gürkaynak, M., & İren, A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 273.

Hagerott, Mark (2014), "Stuxnet and the vital role of critical infrastructure operators and engineers", *International Journal of Critical Insfrastructure Protection*, 7, 244.

Hekim, H. *Oltalama (Phıshıng) Saldırıları*.

Internet Security Threat Report. 2017. Symantec, 22.

İnternet: Coşkun, D. (2018, Mayıs 1). Siber savaş ve siber terör. cio.com.tr: http://www.cio.com.tr/blog/siber-savas-ve-siber-teror/ adresinden alındı

İnternet: European Parliamentary Research Service (2014), Cyber defence in the EU Preparing for Cyber Warfare?, http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143Cyber-defence-in-the-EU-FINAL.pdf (15.03.2016). 2014:5

İnternet: Bircan, B. (2012). docplayer.biz.tr: https://docplayer.biz.tr/1142152-Gelismis-siber-silahlar-ve-tespit-yontemleri-bahtiyar-bircan-uzman-arastirmaci-siber-guvenlik-enstitusu.html adresinden alındı

İnternet: Arslan, Rengin (2015), "Türkiye'ye Siber Saldırının 10 Günü: Ne Oldu?", http://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan (06.02.2016).

İnternet: Alkan, M. (2012). Siber Güvenlik ve Siber Savaşlar. Bilgi Güvenliği Derneği: www.bilgiguvenligi.org.tr/index_files/sunumlar/siber_guvenlik_siber_sava slar_tbmm_internet_komisyonu_mayis_2012.pptx adresinden alındı

İnternet: Arbour Networks, 2017. "Current DDoS attacks", http://www.asiapacificsecuritymagazine.com/w p-content/uploads/2017/01/2017-01-19- Arbor-WISR-Full-Report.pdf

İnternet: 5. Boyutta Savaş: Siber Savaşlar-II, https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html

İnternet: Anonymousdeclares"cyberwar"onIsrael, http://edition.cnn.com/2012/11/19/tech/ web/cyberattack-israel anonymous/index.html

İnternet: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf, Erişim tarihi: 18 Nisan 2019.

İnternet: https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku

İnternet: https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+ countries+ where+attacks-+originate+-++2015.pdf

İnternet: https://www.britannica.com/topic/Trojan-horse Erişim tarihi: 12/11/2019

İnternet: https://www.cisco.com/c/en/us/about/security-center/virus-differences.html Erişim Tarihi: 14.05.19

İnternet: https://www.kaspersky.co.uk/resource-center/threats/viruses-worms Erişim Tarihi 12/11/2019

İnternet: https://searchsecurity.techtarget.com/definition/logic-bomb Erişim Tarihi:12/11/2019

İnternet: https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html Erişim Tarihi: 12/11/2019

İnternet: https://wearesocial.com/global-digital-report-2019 Erişim Tarihi: 12/11/2019

İnternet: https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks Erişim Tarihi: 12/11/2019

İnternet: https://medium.com/@oguzalbastr02/ortadaki-adam-sald%C4%B1r%C4%B1s%C4 %B1-mitm-detayl%C4%B1-anlat%C4%B1m-5e5f86af1d6a Erişim Tarihi: 20.07.2019

İnternet: https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack- Erişim Tarihi 12/11/2019

İnternet: https://www.trustedknight.com/ddos-attacks-3-common-motivations/ Erişim tarihi: 15/11/2019

İnternet: http://www.hurriyet.com.tr/teknoloji/turkiyeye-siber-saldiri-soku-turk-telekomdan-flas-aciklama-geldi-41360791

İnternet: https://www.binance.vision/tr/security/what-is-phishing

İnternet: https://www.phishlabs.com/about/

İnternet: https://www.f5.com/labs/articles/threat-intelligence/2019-phishing-and-fraud-report

İnternet: https://www.egm.gov.tr/bilgiteknolojileri/projeler Erişim Tarihi: 16/11/2019

İnternet: https://veriakademi.com/sql-nedir

İnternet: https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

İnternet: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina /the-great-firewall-of-china-background/index.html

İnternet: http://sozluk.gov.tr/ Erişim tarihi: 19/07/2019

İnternet: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.53ec947c405869.39672886

İnternet: https://www.hsdl.org/?abstract&did=487492 Erişim Tarihi: 19/11/2019

İnternet: https://www.binance.vision/tr/security/what-is-a-51-percent-attack Erişim Tarihi: 13/11/2019

İnternet: https://www.btk.gov.tr/siber-guvenlik-kurulu

İnternet: https://nakedsecurity.sophos.com/2011/08/03/shady-rat-biggest-cyber-attack/ Erişim Tarihi: 13/11/2019

İnternet: https://siberbulten.com/makale-analiz/gelmis-gecmis-en-genis-capli-siber-saldiri-shady-rat/ Erişim Tarihi: 13/11/2019

İnternet: https://21yyte.org/tr/merkezler/bolgesel-arastirma-merkezleri/orta-asya-arastirmalari-merkezi/dar-alanda-buyuk-pazarlik-kirgizistanda-abd-ile-rusyanin-us-mucadelesi Erişim Tarihi: 13/11/2019

İnternet: https://siberbulten.com/makale-analiz/gelmis-gecmis-en-genis-capli-siber-saldiri-shady-rat/ Erişim Tarihi: 13/11/2019

İnternet: Karakuş, C. (2019, Ağustos). Kritik Alt Yapılara Siber Saldırı. ckk.com.tr: http://ckk.com.tr/bilimsel/siber.pdf adresinden alındı

İnternet: McAfee (2011), "Revealed: Operation Shady RAT", http://www.mcafee.com/us/resources/ white-papers/wp-operation-shady-rat.pdf (19.02.2016).

İnternet: Mueller Paul ve Yadegari Babak (2012), "The Stuxnet Worm", http://www.cs.arizona.edu /~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf (01.02.2016).s.10

İnternet: Nye, J. S. (2014, Mayıs). The Regime Complex for Managing Global Cyber Activities. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf adresinden alındı

İnternet: Pamuk, O. (2012, 05 17). Stuxnet'i Özel Yapan Ne? TUBİTAK BİLGEM: http://-www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html adresinden alındı

İnternet: Passeri, P. (2019). 2018: A Year of Cyber Attacks. www.hackmageddon.com: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/ adresinden alındı

İnternet: Rouse, M. (2018, Mayıs). searchsecurity.techtarget.com. techtarget.com: https://searchsecurity.techtarget.com/definition/social-engineering adresinden alındı

İnternet: Smith, Craig S. (2001), "6-12; The First World Hacker War", The New York Times, http://www.nytimes.com /2001/05/13/ weekinreview/may-6-12-the-first-world-hacker-war.html (01.02.2019).

İnternet: Traynor, I. (2019, Temmuz 2). Theguardian.com: https://www.theguardian.com/world/2007/may/17/topstories3.russia adresinden alındı

İnternet: Ukrayna Elektriğine Siber Saldırı-Enerji Günlüğü (2016) http:// enerjigunlugu.net/ukrayna-elektrigine-siber-saldiri_16907.html

İnternet: UK Cabinet Office. "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World", Cabinet Office, <http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategyfinal.pdf>, 17.05.2012.

İnternet: Vinnakota, T. (2013). Understanding of Cyberspace Using Cybernetics: An Imperative need for Cybersecurity of Enterprises. https://ieeexplore.ieee.org/document/6865791 adresinden alındı

İnternet: Yazıcı, A. (2011, Kasım). Güvenli Bilgi Paylaşımı ve SAHAB. emo.org.tr: http://www.emo.org.tr/ekler/fad64faae21db53_ek.pdf adresinden alındı

İnternet: Üneri, M. (2009, Temmuz). Bilgisayar Güvenliği ve Internet. bilgitoplumu.gov.tr: http://bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/090715_IK27.ToplantisiInternetVeBilgisayarGuvenligi.pdf adresinden alındı

John, B. (2008). Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler Dergisi*, 5(18).

Kaban, Z. Y. (1994). GENEL Sistem Teorisi ve Sibernetik. *Marmara İletişim Dergisi*, 219-226.

Kara, M. (2013). *Siber Saldırılar - Siber Savaşlar ve Etkileri*. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Ve Teknoloji Hukuku Yüksek Lisans Tezi. İSTANBUL.

Kartal, A. B. (2014). Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği. *Güvenlik Stratejileri*, 39-77.

Kasapoğlu, C. (2017). *Siber Güvenlik: Beşinci Boyutu Anlamak*. EDAM Siber Politikalar Kağıtları Serisi.

Keleştemur, A. (2015). *Siber İstihbarat*. Level Kitap.

Keleştemur, S. (2018). *Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi*. Gedik Üniversitesi Yüksek Lisans Tezi. İstanbul.

Machievelli Çev. Nazım Güvenç. (2002). *Askerlik Sanatı.* İstanbul: Anahtar Kitapları Yayınevi.

Michael N. S. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 92.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, 140(4), 70-92.

Özocak, G. (2012). DDoS Saldırısı ve Failin Cezai Sorumluluğu. *Bilişim*, 28, 23.

Sağıroğlu, Ş. (2017). Siber Terörle Mücadele : Tehditler ve Önlemler Konferansı. *Siber Terör: Tehditler Ve Önlemler,* (s. 6).

Sezgin, M., & Talaz, L. (2016). Bilişim Devrimi, Sibernetik İletişim ve Stratejik Halkla İlişkiler. *Karabük Üniversitesi Sosyal Bilimler Dergisi*, 559-571.

Sharma, B. (2017). *A Pragmatic Way of Logic Bomb Attack Detection Methodology*. Indian Journal of Science and Technology.

Şahinaslan, Ö. (2013). *Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma*. Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Doktora Tezi. EDİRNE.

Şen Ş. & Akgün F. & Buluş E. Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler Ve Korunma Yollarının İncelenmesi

TBB Raporu. (2006). *Türkiye ve Terörizm*. Ankara: Türkiye Barolar Birliği Yayınları.

Tombul, F., Güneştaş, M., & Başıbüyük, O. (2015). Siber Suçlar; Tehditler,Farkındalık Ve Mücadele. *Global Politika ve Strateji.*

Türkay, Ş. (2013). *Siber Savaş Hukuku ve Uygulanma Sorunsalı*. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 1177-1227.

Ulaştırma ve Altyapı Bakanlığı - 2016-2019 *Ulusal Siber Güvenlik Stratejisi* (2016).

Ulaşanoğlu, M. E., Yılmaz, R., & Tekin, M. A. (2010). *Bilgi Güvenliği: Riskler ve Öneriler*. ANKARA: Bilgi Teknolojileri ve İletişim Kurumu.

Ünver, M. (2011). Ulusal Bilişim Kongresi. *Ulusal SİIber Güvenliğin Sağlanması*. Kayseri.

Virvilis, N., & Gritzalis, D. (2013, September). *The big four-what we did wrong in advanced persistent threat detection?.* In 2013 International Conference on Availability, Reliability and Security (s. 248-254).

Weaver, O. (2004). *Copenhagen New 'Schools' in Security Theory and their Origins between Core and Periphery*. Paris: International Studies Association.

Yalman, Y. (2018). Siber Terör, Terörizm ve Mücadele. Ş. Sağıroğlu, & M. Alkan içinde, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (s. 259). Ankara: Grafiker Yayınları.

Yıldız, M. (2014, Kasım). *Siber Suçlar Ve Kurum Güvenliği*. Denizcilik Uzmanlık Tezi. Ulaştırma Denizcilik Ve Haberleşme Bakanlığı.

Zbigniew Brzezinski Çev Yelda Türedi. (tarih yok). *İkinci Şans*. İstanbul: İkılap Yayınevi.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: POLAT Semih
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 11/09/1990 Tercan
Medeni hali	: Evli
Telefon	: 507 853 2624
e-mail	: semihpolatt@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksek lisans	Ankara Hacı Bayram Veli Üniversitesi	Devam Ediyor
Lisans	Polis Akademisi	2012
Lise	Polis Koleji	2008

İş Deneyimi

Yıl	Yer	Görev
2017-	Elazığ	
2013-2017.	Emniyet Genel Müdürlüğü.	Komiser
2012-2013	Kocaeli	Komiser Yardımcısı

Yabancı Dil

İngilizce (YDS 60)

Hobiler

Seyahat etmek

ankara HBM

ankara HBV

le.ahbv.edu.tr