İZMİR KÂTİP ÇELEBİ ÜNİVERSİTESİ
2010
FEN BİLİMLERİ ENSTİTÜSÜ

Siber Silahların Etkileri Stuxnet ve Duqu Olayları Üzerinde İnceleme Çalışması

Yazılım Mühendisliği Ana Bilim Dalı

Tezsiz Yüksek Lisans Bitirme Projesi

Fikret GÜNGÖR
ORCID 0000-0002-1156-0666

Proje Danışmanı: Prof. Dr. Femin YALÇIN KÜÇÜKBAYRAK

Ocak 2023

İzmir Kâtip Çelebi Üniversitesi Fen Bilimleri Enstitüsü Yazılım Mühendisliği A.B.D. öğrencisi **Fikret GÜNGÖR** tarafından hazırlanan **Siber Silahların Etkileri Stuxnet ve Duqu Olayları Üzerinde İnceleme Çalışması** başlıklı bu çalışma tarafımca okunmuş olup, yapılan inceleme sonucunda kapsam ve nitelik açısından başarılı bulunarak tarafımdan YÜKSEK LİSANS BİTİRME PROJESİ olarak kabul edilmiştir.

ONAYLAYAN:

Proje Danışmanı: **Prof. Dr. Femin YALÇIN KÜÇÜKBAYRAK**
İzmir Kâtip Çelebi Üniversitesi

Yazarlık Beyanı

Ben, **Fikret GÜNGÖR**, başlığı **Siber Silahların Etkileri Stuxnet ve Duqu Olayları Üzerinde İnceleme Çalışması** olan bu projemin ve projenin içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu projenin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Projenin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Kayda değer yardım aldığım bütün kaynaklara teşekkür ettim.
- Projede başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

Tarih: 15.01.2023

Siber Silahların Etkileri Stuxnet ve Duqu Olayları Üzerinde İnceleme Çalışması

Öz

Bu çalışma, Stuxnet ve Duqu'nun etkilerini ve yeteneklerini açıklayarak ve bu yetenekleri karşılaştırarak devlet kaynaklı siber silahların siber güvenlik ve bilgisayar ağı operasyonlarına etkilerini incelemeyi amaçlamaktadır. Literatür tarafından oluşturulan siber silahların tanımları ilk siber savaş olarak tanımlanan Estonya devletine karşı 2007 yılında yapılan dağıtılmış hizmet reddi saldırıları vakası, hizmet reddi saldırılarının siber silahlar olarak sınıflandırılıp sınıflandırılamayacağını anlamak için de incelenmektedir. Stuxnet'in bir siber silahın tanımlarına ve tanımlarına uyduğu tespit edilirken; Duqu, iki devlet aktörü tarafından taşınan kötü amaçlı yazılım arasındaki operasyonel farklılıklar nedeniyle bir casusluk varlığı olarak sınıflandırılmıştır. Estonya'ya yönelik hizmet reddi saldırıları, literatür tarafından oluşturulan siber silah veya siber savaş tanımlarına uymamıştır.

Anahtar Sözcükler: Siber alanlar, siber saldırı, stux-net, duqu

Effects of Cyber Weapons Stuxnet and Duqu And Examination Study on the Incidents

Abstract

This work aims to examine and discuss the implications of state-borne cyber weaponry to cybersecurity and computer network operations through explaining the effects and capabilities of Stuxnet and Duqu and comparing these abilities to the definitions of cyber weapons established by the literature. Heralded as the first cyber war, case of distributed denial of service attacks of 2007 against the state of Estonia is also examined to understand whether denial of service attacks can be classified as cyber weapons. Stuxnet was found to have fit within the descriptions and definitions of a cyber weapon while the Duqu has been classified as an espionage asset due to operational differences between two state actor bornemalware. Denial of service attacks against Estonia did not conform to the cyber weapon or cyber warfare definitions established by the literature.

Keywords: Cyber weapons, Cyber warfare, Stux-net, Duqu

Proje çalışmasına katkılarından dolayı danışmanım Sayın Profesör Doktor Femin YALÇIN KÜÇÜKBAYRAK'a teşekkürlerimi sunarım.

İçindekiler

Tabloların Listesi

Şekiller Listesi

Kısaltmalar Listesi

APT	: Gelişmiş Kalıcı Tehditler
AS	: Otonom Sistemler
BCI	: Beyin Bilgisayar Arayüzü
BGP	: Sınır Ağ Geçidi Protokolü
CCDCOE	: İşbirlikçi Siber Savunma Mükemmeliyet Merkezi
CERT	: Bilgisayar Acil Durum Hazırlık Ekibi
CISA	: Siber Güvenlik ve Altyapı Güvenliği Ajansı
CAN	: Bilgisayar Ağı Saldırıları
CNE	: Bilgisayar Ağından Yararlanma
CNO	: Bilgisayar Ağı İşlemleri
CYBINT	: Siber İstihbarat
DoS	: Hizmet Reddi
DDoS	: Dağıtılmış Hizmet Reddi
DNS	: Alan Adı Sistemi
HIDS	: Ana Bilgisayar Tabanlı İzinsiz Giriş Tespit Sistemleri
HUMINT	: İnsan Zekâsı
HTTP	: Köprü Metni Aktarım Protokolü
HTTPS	: Güvenli Köprü Metni Aktarım Protokolü
IANA	: İnternet Tahsisli Numaralar Yetkilisi
ICS	: Endüstriyel Kontrol Sistemleri
ICT	: Bilgi ve İletişim Teknolojileri
IDS	: İzinsiz Giriş Tespit Sistemi
IEEE	: Elektrik Elektronik Mühendisleri Enstitüsü
IoT	: Nesnelerin İnterneti
IPS	: İzinsiz Giriş Önleme Sistemi

ISP : İnternet Servis Sağlayıcı

IAEA : Uluslararası Atom Enerjisi Ajansı

IT : Bilgi Teknolojileri

IW : Bilgi Savaşı

LAN : Yerel Alan Ağı

MitM : Ortadaki Adam Saldırısı

NIDS : Ağ Tabanlı İzinsiz Giriş Tespit Sistemleri

PPI : Yükleme Başına Ödeme

OSI : Açık Sistemler Arası Bağlantı

OSINT : Açık Kaynak İstihbaratı

OSN : Online Sosyal Ağlar

OSS : Açık Kaynak Kodlu Yazılım

P2P : Eşler Arası

RAM : Rastgele Erişim Belleği

RAT : Uzaktan Erişim Aracı

SCADA : Denetleyici Kontrol ve Veri Toplama

SCM : Tedarik Zinciri Yönetimi

SIEM : Güvenlik Bilgileri ve Olay Yönetimi

TCP/IP : İletim Denetimi Protokolü /İnternet Protokolü

tDCS : Transkraniyal Doğru Akım Stimülasyonu

TMS : Transkraniyal Manyetik Stimülasyon

UDP : Kullanıcı Datagram Protokolü

UID : Benzersiz Tanımlayıcı

USB : Evrensel Seri Veri Yolu

VLAN : Sanal Yerel Alan Ağı

WAN : Geniş Alan Ağı

XSS : Siteler Arası Komut Dosyası Çalıştırma Saldırısı

1.Giriş

Siber uzay gerçek dünyadan farklıdır. Bu ifade hiç kimse için sürpriz olmayabilir, ancak yine de belirtilmesi gerekir. Siber uzayla ilgili yaygın olarak kabul edilen yanlış anlama, vatansız olduğu ve hava gibi aynı anda herkese ait olduğudur. İnternetin soluduğumuz hava kadar önemli olduğu noktasında hemfikir olsam da, siber uzayın vatansız ve sınırsız olduğuna inanmak doğru değil. Siber uzay, sunucuların, yönlendiricilerin, anahtarların ve bilgisayarların fiziksel altyapısında bulunur ve otonom sistemlerden (AS) oluşur. Sınır geçidi protokolü (BGP) rota bağlantılarıyla birbirine bağlanan, sürekli değişen otonom sistemlerin onlarca housand'ı, her zaman herhangi bir bağlantının daha düşük gecikme süresine geçmek için en yakın AS'yi bulmaya çalışmaktadır (Fontugne, et al., 2019, p. 197). Tüm bu physical altyapısı siber uzayı fiziksel aleme bağlar. Bununla birlikte, fiziksel alanın aksine, değişime yönelik eğilim siber uzayın özünde yatmaktadır. İçinde yer alan tüm bilgiler değiştirilebilir. Bu nedenle, siber uzayın kendisi, icadından bu yana bir boyut olarak değişmemiş olabilir, içeriği ve kuralları kesinlikle vardır. P. W. Singer ve Allan Friedman'dan alıntı yapmak gerekirse, "bugünün siber uzayı 1982'deki siber uzayla hem aynıdır hem de tamamen farklıdır" (Singer ve Friedman, 2014, s. 14). Bir kez daha fiziksel dünyanın aksine, devletler siber uzaydaki en güçlü varlıklar değildir. Yeterli teknik uzmanlığa sahip iyi finanse edilen gruplar, bir devlet aktörünün yapabileceğinden daha fazla zarar verebilir, çünkü saldırılar doğrudan kendilerine atfedilemezse, bu gruplar genellikle yasal yankıları engellenmez. Bireyler bile siber uzaydaki bilgisayar ağı operasyonlarını (CNO) bozma, bölümlerine erişimi reddetme veya internetin Darknet adı verilen yeraltı bölgelerinde en güçlü teklif sahibine satmak için sınıflandırılmış bilgileri tamamen çıkarma yeteneğine sahiptir. Ancak siber uzaydaki güç dengesi değişiyor. Dünya, Olimpiyat Oyunları Operasyonu (Sanger, 2012) veya daha yaygın olarak Stuxnet ve daha sonra Duqu lakaplı casusluk odaklı varyantı olarak adlandırılan özel bilgisayar ağı saldırılarının (CNA) etkilerini gördü. Dahası, hedeflenen siber saldırılar ve gelişmiş kalıcı tehditler sürekli olarak gelişiyor, milyonlarca endüstriye mal oluyor ve siber uzaydaki ilişkilendirme sorunları nedeniyle, saldırganlar pratik olarak bundan kurtuluyorlar.

1.1 Proje Kapsamı

Bu projede, öncelikle siber uzayın tanımlarını ve siberden türetilen terimlere uygun olarak devlet ve devlet dışı aktörlere yönelik siber tehdit türlerini inceledim. Bu belirlenen hedefi takiben, Stuxnet ve varyantı Duqu gibi devlet aktörlerine karşı önde gelen hedefli siber saldırı vakalarını ve Estonya'ya karşı ne tür hedefli ve hedefsiz siber saldırılar gerçekleştiğini ve saldırı vektörlerini tanımlayan ünlü hizmet reddi saldırısını da inceledim ve Gelecek için bu tür saldırılara karşı önlemler önermeye gayret ettim.

Proje kapsamını sınırlamak için, hedefli ve hedefsiz siber saldırıların yanı sıra gelişmiş kalıcı tehditler (APT) yalnızca teknik bir bakış açısıyla incelenmektedir. Literatür araştırmaları, siber uzayın bilgisayar bilimlerinden uluslararası ilişkilere ve uluslararası hukuka kadar uzanan çok disiplinli bir alan olduğunu göstermektedir. Literatür araştırmaları ayrıca, uluslararası ilişkiler alanında gelişmiş kalıcı tehditler ve devlet kaynaklı siber silahlarla ilgili teknik anlayış ve inceleme eksikliğine işaret etmektedir. Bu nedenle, bu proje, hedefli ve hedefsiz siber saldırılar, terimler ve saldırı vektörleri, yayılma teknikleri ve bu tehditlere karşı bazı basit karşı önlemlerin yüzeysel bilgisinin sadece bireylere fayda sağlamakla kalmayıp, aynı zamanda herhangi bir güvenli alanda olduğu gibi devlet güvenliğini de etkileyebileceğini ortaya koymaya çalışmaktadır. ağ, kesmek için en kolay bileşen insan unsurlarıdır. Daha önce belirlenen sınırları takiben, bu proje siber saldırılar ve siber savaşla ilgili uluslararası hukuku incelememekte ve sadece bilgisayar bilimleri ve uluslararası ilişkilerin bakış açılarını dikkate almaktadır.

1.2 Amaç

Bu projenin amacı, siber uzayın devlet ve devlet dışı aktörleri kapsayan çok yönlü ve çok disiplinli bir küresel alan olduğu fikrini ortaya koymaktır. Siber uzayla ilgili uluslararası ilişkiler alanında yapılan önceki çalışmaların aksine, bu proje siber uzay ve bilgi iletişim teknolojilerinin (BİT) tekniklerinden uzak durmuyor. Uluslararası ilişkiler ve devletler öyle yeni ufuklara doğru ilerliyor ki, kara, deniz, hava, uzay ve siber olmak üzere beş geleneksel alan kendi alanlarıyla sınırlı kalmıyor.

artık sınırlar. Günümüzde ordular, kuvvet yansıtmak ve taktik yeteneklerini göstermek için alanlar arası manevralar kullanıyor. Basitçe söylemek gerekirse, uluslararası sularda konumlandırılmış bir taşıyıcıdan çalışan bir drone, bilgisayar güdümlü bir füze konuşlandırırken, çok sayıda veriyi uzak bir bilgisayara iletir. yörüngedeki uydular, alanlar arası manevralar teriminin neyi iletmeye çalıştığını açıklamak için mükemmel bir örnektir. Bu yörüngeyi genişleterek, bu çalışma, Uluslararası İlişkiler alanında uzman olmak için, operasyonel alanlardan birini inceleyen çizgiler boyunca formüle edilmiştir. Etki alanları, basit ordu terimlerinden operasyonel bilgisayar ağı altyapılarına kadar tüm alanlardaki tüm terimleri ve anlamlarını kavrayabilmelidir. Ana akım teorilerin başarısız olduğu göz önüne alındığında Sovyetler Birliği'nin çöküşünü öngörmek ve uluslararası ilişkiler alanında zorlanmıştır.

Sovyetler Birliği'nin çöküşünün ardından meydana gelen paradigma değişimlerine ikna edici açıklamalar sunmak için yeni bir teori ortaya koyan bu proje, bu nedenle, Bu ana akım teoriler, ana konusunu incelerken ve açıklarken dikkate alınır: devlet aktörlerine karşı silahlandırılmış kötü amaçlı yazılım kullanan hedefli ve hedefsiz siber saldırılar.

Aşağıdaki bölümler, siber saldırıların saldırgan tarafından belirlenen bir hedefe ulaşmak için silahlandırılmış kötü amaçlı yazılım kullandığını açıklayacak ve bu silahların nasıl çalıştığını inceleyecek ve açıklayacaktır. Bu silahların yarattığı güvenlik etkilerini ve zorlukları daha iyi anlamak için, silahlandırılmış kötü amaçlı yazılım saldırı vakaları, yani Stuxnet ve varyantı Duqu vakaları bu projenin ana odağı olacaktır. Bu proje, siber alanda faaliyet gösteren herhangi bir devlet veya devlet dışı aktörü siber savaşçılar olarak töhmet altında bırakmaya çalışmaz, saldırganlar terimi basitçe söz konusu silahlandırılmış kötü amaçlı yazılımı tohumlayan bir d tohumu oluşturan geniş kurumsal ve kurumsal olmayan varlıklara atıfta bulunmak için bir zamir olarak kullanılır.

Bu proje, devletlerin siber güvenlik eğitimine odaklanmadığını varsaymaktadır. Bu da siber savunma stratejilerini cansız bırakıyor ve güvenlik alanında güvenliğin sürekli değişen yönlerine çözüm sunamıyor. Bu öncül üzerine inşa edilen bu proje, siber silahların artık bir gerçeklik olduğunu ve siber alemde bulunan yaygın kötü amaçlı yazılımlardan gerçekten farklı olduklarını varsaymaktadır. Şu anda devletlerin siber silah kabiliyetleri bilinmemektedir ve bu konuda daha fazla araştırma yapılmadan, geliştirilen siber silahlara karşı siber savunma politikalarının sağlanması mümkün olmayacaktır. hem devlet hem de devlet dışı aktörler tarafından konuşlandırılır. Son olarak, bu proje, siber uzayda güvenliğin devam eden bir süreç olduğunu, yani hiçbir sistemin tamamen güvenli olamayacağını varsaymaktadır.

1.3 Anahat

Bölüm 2, siber ve türev terimleri, ilgili konularda literatür araştırması yoluyla tanımlamaktadır.

Bölüm 3, hedeflenen ve hedeflenmeyen siber tehditlerin yönlerini belirlemeye odaklanmaktadır. Bölüm 4, bugüne kadar daha belirgin siber saldırılardan bazılarının vaka çalışmalarını incelemektedir. Bölüm 5, en yüksek siber politikalardan bazılarında kullanılan mevcut siber politikaları incelemektedir.

savunmasız ulusların yanı sıra uluslararası örgütler.

Bölüm 6, Beyin Bilgisayar Arayüzleri (BCI) ve artırılmış gerçeklik gibi ilerlemeler yoluyla insan yaşamında siber uzay entegrasyonunu artıran gelecekteki senaryoların bazılarını formüle etmekte ve araştırmakta ve projeyi sonuçlandırmaktadır.

2.Tanımlar

Siber güvenlik, Uluslararası İlişkiler alanında oldukça yeni bir konudur. Konu, bilgi teknolojileri ve bilgisayar bilimleri alanlarında aktif ve sağlıklıdır, çünkü küresel ağlarda yayılan muazzam hız ve saldırılar nedeniyle, birçok uzman bilgi iletişim teknolojilerinin her biçimini yetkisiz erişim, kurcalama veya modifikasyondan korumak için çaba göstermektedir. Uluslararası ilişkiler alanının bakış açısından,siber güvenlik teriminin ne anlama geldiği hala yeterince açık değildir. Literatür araştırmaları, siber güvenliğin hemen hemen her araştırmacı ve devlet tarafından farklı şekilde tanımlanmakla kalmayıp, aynı zamanda siber uzayı, siber silahları, siber savaşı ve siber taktikleri de etkilediğini göstermektedir. Projenin bu bölümü, literatürdeki tanımları karşılaştırarak yukarıda belirtilen konuları çevreleyen karışıklığın bir kısmını gidermeyi amaçlamaktadır.

Bu çalışmanın başında, siber uzayın ne olduğunu sıfırdan inşa etmek faydalı olacaktır. Siber uzayın ne olduğu, nerede var olduğu ve bu temelin üstünde yer alan gerçek dünyayla nasıl etkileşime girdiği, siber güvenlik, siber savaş, siber suçlar ve siber saldırılar gibi alt unsurları açıklanabilir. Bununla birlikte, Uluslararası İlişkiler alanında, Sovyet Sosyalist Cumhuriyetler Birliği'nin (SSCB) çöküşünden sonra güvenlik terimiyle kastedilen şey, insan güvenliği teriminin giderek daha fazla kullanılmasıyla odağı kademeli olarak devletten bireye kaydıran bir değişime uğramıştır. Bu değişim aynı zamanda siber güvenlik konusunda farklı bir bakış açısı yaratıyor, bir siber saldırının hedefi devlete ait bir kurum veya altyapı olsa da, askeri savaşla benzerlikler taşıyor olsa da, çoğu zaman en çok etkilenen bireylerdir. Gelecek bölümlerde bu proje siber saldırıları derinlemesine incelemektedir. Bununla birlikte, referans niteliğindeki

güvenlik nesnesinin devletlerden bireylere kaymasıyla birlikte, bu proje aynı zamanda siber uzaydaki bireylerin güvenliğini de tartışacaktır.

2.1 Siber Uzay

Siber terimi, Eski Yunanca bir fiil olan κυ βερεω (kybereo) 'dan türetildiği inancının ötesinde kendi başına çok az anlam ifade eder, "yönlendirmek, rehberlik etmek, kontrol etmek ya da yönetmek" (Yan, 2019, s. 1). Siberin mevcut sözlük tanımı: "bilgisayarlarla veya bilgisayar ağlarıyla (internet gibi) ilgili veya bunlarla ilgili". Sibere gerçek anlamını veren şey, birlikte kullanıldığı şu kelimelerdir: uzay, savaş veya saldırı.

Siber uzay terimi, William Gibson'ın "Neuromancer " adlı romanıyla popüler hale geldi. Bu terimi "Burning Chrome" adlı önceki çalışmasında kullanmış olsa da, Neuromancer'daki siber uzay tanımı, siber uzay teriminin özünü yakalayan şeydir.

"Siber uzay. Her gün milyarlarca meşru operatör tarafından, her ulusta, çocuklara matematiksel kavramların öğretilmesiyle yaşanan rızaya dayalı bir halüsinasyon... İnsan sistemindeki her bilgisayarın bankalarından soyutlanan verilerin grafik bir temsili . Düşünülemez karmaşıklık. Işık çizgileri zihnin uzayında, kümelerinde ve veri takımyıldızlarında değişiyordu. Şehir ışıkları gibi, geri çekiliyor..." (Gibson, 1984, s. 51)

Her yıl ve ulustaki milyarlarca günlük meşru kullanıcı, dünya çapında farklı bilgisayar sistemlerinden oluşturulan karmaşık verilerin grafiksel temsili ile etkileşime girerek,

ve günümüzde cebimizde taşıyabileceğimiz en küçük ekranlarda bile sergilenen, ne kadar mecazi gelse de, siber uzayın özünde, bir veri boyutunda neyi temsil ettiğinin uygun bir açıklamasıdır; ona bağlı her cihaz bir ağ geçidi ve bir kahin görevi görür. Karmaşık baytları insan sarf malzemesi formuna şekillendirmek ve yönlendirmek.

Literatürdeki pek de mecazi olmayan tanımlara geri dönersek, Richard Clarke ve Robert Knake'nin siber uzay tanımı "dünyadaki tüm bilgisayar ağları ve bağladıkları ve kontrol ettikleri her şey... siber uzay, İnternet'i ve İnternet'ten erişilememesi gereken birçok ağı içerir "(Clarke ve Knake, 2010,

s. 70). Siber uzay, internete bağlı olsun ya da olmasın tüm bilgisayar ağlarını kapsarken, Clarke ve Knake'nin tanımını açıklığa kavuşturmak için, bilgisayar sisteminin var olması siber uzayda, internete ait olmaları gerekmez. Aslında, İnternet siber uzayın bir alt kümesidir, metaforik olarak, bilgisayarların atanmış d İnternet Protokolü (IP) adresleri aracılığıyla tanımlandığı, bu yer imlerinin markalandığı alan adlarıyla hatırlandığı, hepsinin Alan Adı Sunucusu (DNS) Kökü, İnternet Atanmış Sayılar Otoritesi sınırları içinde tutulduğu bir yer imleri koleksiyonudur. (IANA). İnternet yalnızca iki bilgisayar sistemi arasındaki bağlantıyı

kolaylaştırır.

Sonunda İnternet'e giren ARPANET'in yaratıcısı olarak bilinen Amerika Birleşik Devletleri Savunma Bakanlığı (DOD), siber uzayın ne olduğunu tanımlamakta da zorlandı ve 2006 yılında siber uzay tanımlarını aşağıdakilerle genişletti:

> " İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü süreçler ve denetleyiciler dahil olmak üzere birbirine bağlı bilgi teknolojisi altyapıları ağından oluşan bilgi ortamında küresel bir alan" (Mazanec ve Thayer, 2015, s. 13).

P. W. Singer ve Allan Friedman, siber uzayı daha basit terimlerle tanımlar: "Siber uzay, bilginin depolandığı, paylaşıldığı ve çevrimiçi olarak iletildiği bilgisayar ağlarının (ve arkasındaki kullanıcıların) alanıdır" (Singer ve Friedman, 2014, s. 13).

Daha teknik olsa da, basit spektrumun diğer ucunda Daniel Kuehl siber uzayı şöyle tanımlar:

> "Oluşum ortamında, ayırt edici ve benzersiz karakteri elektronik ve elektromanyetik kullanımıyla çerçevelenen küresel bir alan bilgi iletişim teknolojilerini kullanarak birbirine bağımlı ve birbirine bağlı ağlar aracılığıyla bilgi oluşturmak, depolamak, değiştirmek, değiştirmek ve istismar etmek için spektrum." (Robinson, Jones ve Janicke, 2015, s. 72)

Bu projenin hedeflerinden biri siber uzay hakkında teknik arka plan sağlamaktır ve Kuelh'in siber uzay tanımı, multidisipliner siber uzay ve siber güvenlik alanında yer alan herkes için yeterince açıktır. Terimin farklı literatürden daha fazla diseksiyonu sadece suları bulandırmaya hizmet edecektir ve bu nedenle bu proje, Kuehl'in tanımını bu çalışmanın geri kalanı için siber uzayın tanımı olarak kabul etmektedir.

Tablo 2.1, bu bölümde ele alınan bazı tanımları ve literatürde bulunan ve yukarıda tartışılmayan diğer bazı tanımları özetlemeye çalışmaktadır.

Yazar	**Tanımlama**
Clarke and Knake	Tüm bilgisayar ağlarına bağlanılabilir ve kontrol edilebilir
US DoD	Bilgi ortamının küresel etki alanı BT altyapısının birbirine bağlı ağlarıdır
Singer and Friedman	Bilgi depolama paylaşma ve iletişim kuran bilgisayar ağlarıdır
Alison Lawlor Russell	Siber uzay gerçekleşecek bilgi etkileşimlerin yarattığı kullanılabilir bir elektronik fiziksel alandır.
Kuchl	Küresel bir bilgi depolama alanı oluşturma için elektronik ve elektromanyetik olarak birbirine bağlı ağlarda değişiklik yapmak, veri alışverişi yapmak.

2.2 Siber Silahlar

Bir silahın sözlük tanımları (1) "bedensel zarar veya fiziksel zarar vermek için tasarlanmış veya kullanılan bir şey" ve (2) "bir avantaj elde etmenin veya kendini savunmanın bir aracıdır. bir çatışma veya yarışma" . İnsanlara verilen fiziksel zararın veya siber ortamdaki silahların altyapı gereksiniminin aksine, yalnızca sızmış sistemlerde veri bütünlüğünü değiştirme yeteneğine sahip olanlar silah olarak sınıflandırılabilir. Bununla birlikte, bu noktaya kadar, işlenen eylemlerle doğrulanmış bir bedensel zarar veya yaşam kaybı vakası olmamıştır.

siber uzayda bilgisayar kodu. Bu tanıma göre, hedeflenen siber saldırıların ve gelişmiş kalıcı tehditlerin çoğu sadece casusluk araçlarıdır ve siber silahlar olarak sınıflandırılmamıştır. Jacqueline Eggenschwiler ve Janje Silomon "Siber silah normu ve yapımındaki zorluklar ve fırsatlar" başlıklı çalışmalarında, Thomas Rid ve Peter McBurney'nin siber silah tanımını "amaçla kullanılan veya kullanılmak üzere tasarlanan bilgisayar kodu" olarak bildirmektedir. yapılara, sistemlere, canlılara fiziksel, işlevsel veya zihinsel zarar vermek veya tehdit etmek" (Eggenschwiler ve Silomon, 2018, s. 12). Bu thesis, veri bütünlüğüne, fiziksel olarak bağlı cihazlara ve / veya operatörlerine veya bağımlılarına zarar vermeyi amaçlayan bir toplama bilgisayar kodu olan bir siber silah tanımını benimser.

Literatür araştırmaları, siber silahların kıyamet getirebileceği veya buna çok yaklaşabileceği inancının Uluslararası İlişkiler alanında oldukça yaygın olduğunu göstermektedir. Richard Clarke ve Robert Knake, "siber savaşçılar bu ağlara girebilir ve onları kontrol edebilir veya çökertebilir. Bir ağı ele geçirirlerse, siber ve arriorlar tüm bilgilerini çalabilir veya para taşıyan, petrol döken, gaz tahliye eden, jeneratörleri havaya uçuran, trenleri raydan çıkaran, uçakları çarpan, müfrezeyi pusuya düşüren veya bir füzenin yanlış yerde patlamasına neden olan talimatlar gönderebilir "(Clarke ve Knake, 2010, s. 70). İlk önce Clarke ve Knake tarafından boyanan bir ağ saldırısının kasvetli görünümündeki en yıkıcı öngörüye odaklanarak, füze yolunu tek başına değiştirmek, askeri donanıma kapsamlı bir iç bilgi gerektirecek ve hatta kaynak koduna erişim gerektirebilir. Stuxnet örneğinde, silah, gaz santrifüjleri kelimenin tam anlamıyla kontrolden çıkarken, operatörleri ve mühendisleri yanlış bir anlamda güvenlik anlamında sakinleştirirken, izleme istasyonuna geri bildirilen verileri yakaladı ve değiştirdi. Programlanabilir mantık denetleyicilerinin (PLC) izleme işlevini içerdiği kodla değiştirerek bu görevi yerine getirebildi (Falliere, O Murchu, and Chien, 2011, p. 36). Stuxnet'i Clarke ve Knake'de açıklanan füze senaryosuyla karşılaştıran bir saldırganın, füze kontrolünü manipüle etmek, en güvenli ve incelenmiş ağ türlerinden birine kötü amaçlı yazılım ile internete bağlanması ve bu fırsatı beklemek için sorumlu kodu bilmesi gerekir. Uçuş sırasında bir füzenin kontrolünü ele geçirmek ve vurmak için an. Stuxnet'in

kuruluşundan bu yana geçen 10 yılda, kötü amaçlı yazılım karmaşıklığı ve gizli saldırı vektörleri arttı, ancak henüz priveya koda erişim olmadan füze yollarını değiştirebilme noktasına gelmedi. bilgisayar güdümlü füze sisteminin çalışmasından sorumludur.

Clarke ve Knake tarafından açıklanan senaryolardan birine yaklaşırken, siber sabotaj nedeniyle bildirilen bir dökülme vakası olmuştur. Clarke ve Knake tarafından tarif edildiği gibi tam olarak bir petrol sızıntısı olmasa da, Vitek Boden, intikam amacıyla yerel parklara, nehirlere ve hatta bir otele bir milyon litreden fazla ham kanalizasyon dökebildi. Queensland / Avustralya'daki Maroochy Shire kanalizasyon pompalarına ve arıtma tesislerine denetleyici kontrol ve veri toplama (SCADA) sistemlerini kuran şirketin çalışanı olduğunu ve bu nedenle söz konusu SCADA sistemlerinin nasıl işletildiğine dair önceden içeriden bilgi sahibi olduğunu belirtmek gerekir. Boden'in revenge komplosu milyonlarca litre ham kanalizasyon dökmüş olabilir, ancak siber silahlar geliştirmek ve konuşlandırmak yerine 150 pompa istasyonunun kontrolünü ele geçirmek için bu görevi yalnızca dizüstü bilgisayarı ve radyo ekipmanıyla yerine getirmişti (Rid ve McBurney, 2012, s. 10).

Bir devlete karşı konuşlandırılacak en etkili siber silahlardan birinin Stuxnet olduğu biliniyor. Son derece seçici hedefleme, teminat hasarına eğilim göstermeden birleştiğinde, onu bugüne kadarki en akıllı siber silahlardan biri yapan şeydir. Bununla birlikte, Stuxnet aslında akıllı bir yazılım parçası değildir, öğrenmek için tasarlanmış diğer birçok yazılımın aksine, Stuxnet öğrenemedi, hedeflerini seçmek ve enfeksiyon rutinlerini başlatmak için önceden ayarlanmış parametreleri kullandı. Bu öngörülebilirlik, siber silahların tali hasarını sınırlayan şeydir, çünkü enfeksiyon zincirindeki bir kırılma kötü amaçlı yazılımı çalışmaz hale getirebilir. Alandaki güvenlik araştırmacıları, kendi kendine öğrenen kötü amaçlı yazılımların ortaya çıkışını tahmin ediyorlar. Küresel bir güvenlik uzmanıolan Derek Manky, kendi kendine öğrenen siber saldırıların 2018 gibi kısa bir sürede gerçeğe dönüşebileceğini öngörmüştü. Manky'ye göre, geleneksel botnet'lerin yerini, diğerlerini hedefleyebilen ve tehlikeye atabilen tehlikeye atılmış cihazların akıllı kümeleri olan hivenets ve swarmbot'lar alabilir. kendi kendine öğrenme yeteneklerine sahip savunmasız sistemler. Bunu genişleten Manky, otomatik güvenlik açığı algılamasına dayalı olarak zaten var olan bilgisayar tarafından oluşturulan kötü amaçlı yazılımların, üretmek için yapay zeka e (AI) kaynakları tarafından geliştirilebileceğini de bildirmektedir. halihazırda mevcut olan güvenlik sistemlerinden kaçmak için ek kötü amaçlı yazılım varyasyonları (Manky, 2017).

2.3 Siber Savaş

Literatür araştırmaları, bir terim olarak siber savaş kavramı için çeşitli tanımlar ortaya koymaktadır. Savaşın genellikle uluslararası ilişkiler ve uluslararası hukukun bir alanı olduğu göz önüne alındığında, bu bölüm bu alanlardaki araştırmacılar tarafından sağlanan tanımlara odaklanmaktadır. Sonraki bölümler

Siber saldırıların ağlara sızma ve verileri ayrıntılı olarak değiştirme veya sızdırma yollarını araştıracak, ancak şu ana kadar, Şart'a göre silahlı bir saldırı olarak da oluşabilecek siber saldırılar yoluyla herhangi bir can kaybı yaşanmamıştır. Birleşmiş Milletler.

Jon R. Lindsay, "Stuxnet ve Siber Savaşın Sınırları" adlı çalışmasında, siber savaşı "bilgisayar ağı saldırılarını bir rakibin fiziksel altyapısını siyasi kazanç için bozmak için bir güç kullanımı olarak kullanan" bir eylem olarak tanımlamaktadır. Buna, savaş zamanında entegre bir saldırıyı kolaylaştırmak için düşman veri işlemesini bozan askeri siber operasyonlar da dahildir" (Lindsay, 2013, s. 372).

Richard Stiennon'un devlet aktörü perspektifinden siber savaş tanımı şöyledir :

> "Siber savaş, başka bir devletin güvenliğine ciddi bir tehdit oluşturan siber uzayda (veya önemli devlet yönlendirmesi veya desteğine sahip devlet dışı aktörler) alınan eylemler veya bir devletin güvenliğine yönelik ciddi bir tehdide (fiili veya algılanan) yanıt olarak alınan aynı nitelikteki bir eylemle politikanın genişletilmesidir" (Stiennon, 2015, s. 8).

Bu tanım, devletler tarafından desteklenmeleri veya çok iyi finanse edilmeleri koşuluyla devlet dışı aktörleri içerir. Darknet çevrelerinde satılan Sıfır Gün (0 günlük) güvenlik açıkları için fiyat aralıklarının 1.000 doların altından 100.000 doların üzerine kadar değiştiği göz önüne alındığında, Stuxnet tipi bir siber silah geliştirmenin maliyeti yüksektir. ve 0 günlük güvenlik açıkları keşfedildikten sonra, daha sonra yamalanırlar, böylece silahın saldırı vektörleri ortadan kaldırılır. Günümüzde nükleer programların çekiciliği, Nükleer Silahların Yayılmasını Önleme Antlaşması'ndan sonra bile, devletlerin caydırıcılık aracı olarak tek kullanımlık silahlar geliştirmekten çekinmediklerini göstermektedir. Bununla birlikte, atom bombalarının aksine, bir siber silah sadece devlet aktörleri tarafından değil, aynı zamanda yeterli teknik uzmanlığa sahip devlet dışı aktörler tarafından da tersine çevrilebilir. Ancak bu, her siber silahın daha fazla silah için bir plan olarak kullanılabileceği şeklinde alınmalıdır. Aşağıdaki bölümler, bazı kötü şöhretli siber silahların nasıl çalıştığını incelemekte ve her siber silahın etkili bir şekilde yalnızca sızmak veya sabote etmek için tasarlananlara karşı olduğunu iddia etmektedir.

Bu çalışma uluslararası ilişkiler alanının sınırları içinde tamamlandığından, Stiennon'un siber savaş tanımı, siber savaşın gereksinimlerini iletmede çok açıktır. Bu proje,

topyekün bir siber savaşın patlak verip veremeyeceği konusunda spekülasyon yapmayı amaçlamamaktadır.

2.4 Siber Suç

Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC), Genel Kurul'un 65/230 sayılı kararını ve Suç Önleme ve Ceza Adaleti Komisyonu'nun 22/7 ve 22/8 sayılı iki kararını takiben, siber suçları "siber bağımlı" gibi geniş terimlerle tanımlayarak üye devletlere siber suçlarla ilgili konularda yardımcı olmaya çalışmaktadır. "Siber etkin" suçlar, belirli suç türleriyle birlikte, yani "çevrimiçi çocuk cinsel istismarı ve istismarı". Bu açıklamalara dayanarak, UNODC "siber bağımlı suçların bir Bilgi İletişim Teknolojileri (BİT) altyapısı gerektirdiğini ve genellikle kötü amaçlı yazılımların oluşturulması, yayılması ve dağıtılması olarak nitelendirildiğini, fidye yazılımları, kritik ulusal altyapıya yönelik saldırılar (örneğin, bir organize suç grubu tarafından bir enerji santralinin siber alıcısı) ve bir web sitesini verilerle aşırı yükleyerek çevrimdışı hale getirme (DDOS saldırısı)". İkincisi, UNODC siber etkin suçu "suç, çevrimdışı dünyada meydana gelebilen, ancak BİT tarafından da kolaylaştırılabilen suçtur. Bu genellikle çevrimiçi dolandırıcılıkları, çevrimiçi uyuşturucu alımlarını ve çevrimiçi kara para aklamayı içerir ". Son olarak, UNODC "çocuk cinsel sömürüsü ve istismarı, açık internette, Darknet forumlarında istismarı ve giderek artan bir şekilde, cinsel çarpıtma olarak bilinen gasp yoluyla kendi yarattığı görüntülerin sömürülmesini içerir" kabul etmektedir.

2.5 Siber Saldırılar

Uluslararası hukuk ve Uluslararası İlişkiler alanları açısından bakıldığında, saldırı terimi karmaşık bir konudur. Gerçekten de, Birleşmiş Milletler bile, başlangıçta Birleşmiş Milletler Şartı'nı hazırlarken "saldırı" terimini tanımlamaya çalışmadı. Birleşmiş Milletler Şartı'ndan meşru müdafaa ile ilgili aşağıdaki alıntı, bir 'silahlı saldırı' sırasında şu sözlerle güç kullanımına izin vermektedir:

"Bu durumda hiçbir şey, Güvenlik Konseyi uluslararası barış ve güvenliği korumak için gerekli önlemleri almadıkça, Birleşmiş Milletler Üyesine karşı silahlı bir saldırı meydana gelirse, bireysel veya toplu meşru müdafaa hakkını zedeleyemez. Bu meşru müdafaa hakkının kullanılmasında Üyeler tarafından alınan tedbirler derhal Güvenlik Konseyi'ne bildirilecek ve bu Şart uyarınca Güvenlik Konseyi'nin uluslararası barış ve güvenliğin korunması veya muhafazası için gerekli gördüğü herhangi bir zamanda böyle bir eylemde bulunma yetki ve sorumluluğunu hiçbir şekilde etkilemeyecektir"

Birleşmiş Milletler Şartı'na göre, meşru müdafaa veya daha spesifik olarak, misilleme amaçlı güç kullanımı, silahlı bir durumda devletlerin doğal olarak sahip oldukları bir şeydir.

Saldırı ve herhangi bir eylem Güvenlik Konseyi'ne bildirilmelidir. Fiziksel alanın sınırları içinde, silahlı bir saldırıya atfetmek, yasadışı savaşçılar ve vekalet savaşı hariç, genellikle hemen mümkündür. Bununla birlikte, siber saldırıların, misilleme gücünün kullanılmasına izin verecek herhangi bir kesinlik derecesiyle atfedilmesi neredeyse imkansızdır. Atıf sorunu, siber uzaydaki tüm verilerin manipüle edilebileceği daha önce bahsedilen gerçekle birleştiğinde, hiçbir devlet, siber uzaydan kaynaklanan sağlam kanıtlar olmadan bu durumu güvenilir bir şekilde suçlayamaz.

Estonya'nın düşmanları, Estonya'nın siber uzay bağımlılığını, 2007'nin kader baharında üç hafta boyunca bilgi, medya ve finans ile yönetişim hizmetlerini neredeyse sakat bırakacak kadar sömürmüştü. Bu olayların ardından NATO, Estonya, Tallinn'de bulunan "İşbirlikçi Siber Savunma Mükemmeliyet Merkezi" (CCDCOE) adlı bir siber komuta girişimi düzenlemiştir. Bu girişimin en belirgin çıktılarından biri, " Siber Operasyonlara Uygulanabilir Uluslararası Hukuk Üzerine Tallinn El Kitabı" ve bu çalışmanın "Uluslararası Tallinn El Kitabı 2.0" başlıklı aşağıdaki "yükseltme " idi. Siber Operasyonlara Uygulanacak Kanun". Bu çalışma kılavuzlarının sadece kılavuzlar olduğu ve herhangi bir NATO üyesi için bağlayıcı olmadıkları unutulmamalıdır. El kitabı, siber saldırıyı "ister saldırgan ister savunmacı olsun, insanlara yaralanma veya ölüme veya nesnelere zarar vermesi veya tahrip olmasına neden olması makul olarak beklenen bir siber operasyon" olarak tanımlamaktadır (Schmitt ve Vihul, 2017, s. 415). Şimdiye kadar, bildirilen insan hayatı kaybı ile herhangi bir siber saldırı olmamıştır, ancak bu projenin bölümlerinden birinin tartıştığı ve formüle ettiği gibi, siber entegrasyon nihayet siber saldırıların mevcut durumu göz önüne alındığında, bu tanımın ortaya çıkmasını sağlayabilir. birkaç ekleme ile güncellenmesi gerekiyor. Daha önceki bölümlerde daha önce tanımlandığı gibi, veri bütünlüğünü kurtarmak, değiştirmek veya başka bir şekilde zarar vermek için bir siber silah konuşlandırılabilir. Elde taşınan iletişim cihazlarının veya akıllı telefonların icat edilmesi ve çoğalmasından sonra, insan-veri etkileşimi en yüksek seviyelere ulaşmıştır. Bu en yüksek etkileşim seviyeleri göz önüne alındığında, veri içeren veya işleyen tüm sistemler için veri bütünlüğüne yönelik tehditler ve saldırılar da bu terimin sınırları içinde dikkate alınmalıdır. Bu çalışmanın geri kalanında, ortaya konan bu noktalardan yola çıkarak, bir siber saldırının tanımı şu şekilde değerlendirilecektir: "İnsanları yaralamak veya sonlandırmak, nesnelere zarar vermek veya yok etmek, veri bütünlüğüne zarar vermek, değiştirmek, yok etmek veya istismar etmek için saldırgan veya savunmacı bir şekilde yürütülen bir siber operasyon.”

2.6 Siber Güvenlik

Literatür araştırması, siber güvenlik terimi için şaşırtıcı sonuçlar vermektedir. Uluslararası İlişkiler araştırmacıları genellikle devletleri siber güvenlik terimi için referans nesnesi olarak görürler ve daha önce "caydırıcılık" gibi alandaki taklit teorilere başvurmaya çalışırlar. Bu projenin hedefleriyle

bağlantılı olarak, siber saldırılara karşı yüzde yüz etkili çözümün tüm bilgisayarları kapatmak ve bir daha asla teknolojik olarak uzaktan bir şey çalıştırmamak olduğu belirtilmelidir. Bu önlemlerin ötesinde, İnternet'in küresel olarak bağlantılı doğasında siber güvende kalmanın başka etkili bir yolu yoktur. Teknoloji gelişmeye ve güncellenmeye devam ettiği sürece, hiçbir sistemin siber uzayda yüzde yüz güvenli olmayacağı kesin olarak söylenebilir.

George Christou, "Avrupa Birliği'nde Siber Güvenlik Esnekliği ve Yönetişim Politikasında Uyarlanabilirlik" başlıklı çalışmasında, Avrupa Birliği'nin siber güvenlik tanımını AB Siber Strateji Belgesi'nden şöyle aktarmaktadır:

> "Hem sivil hem de askeri alanlarda, siber alanı, birbirine bağlı ağları ve bilgi altyapısıyla ilişkili veya zarar verebilecek tehditlerden korumak için kullanılabilecek önlemler ve eylemler. Siber güvenlik, ağların ve altyapının kullanılabilirliğini ve bütünlüğünü ve bunların içerdiği bilgilerin gizliliğini korumaya çalışır" (Christou, 2016, s. 7).

2010 yılında, "Askeri Hizmetler Şefleri, Muharip Komutanlıklar Komutanları ve Müşterek Kurmay Müdürlükleri Müdürleri" için gönderilen bir memorandum, Genelkurmay Başkanlarını sürekli değişen siber uzayla hızlandırmak için neredeyse tüm siber terimlerin sözlüğünü içermektedir.

"Bilginin her türlü (elektronik, fiziksel) güvenliğine ve suça karşı korunmak için alınan önlemler de dahil olmak üzere, bilginin depolandığı, erişildiği, işlendiği ve iletildiği sistemlerin ve ağların güvenliğine karşı tehlike ve riskten kurtulmayı sağlamak için gerekli tüm organizasyonel eylemler, saldırı, sabotaj, casusluk, kazalar ve başarısızlıklar. Siber güvenlik riskleri, paydaş güvenine ve güvenine zarar veren, müşterinin elde tutulmasını ve büyümesini etkileyen, müşteri ve ortak kimliğini ve gizlilik korumalarını ihlal eden, ticari işlemleri yürütme veya yerine getirme, sağlığı olumsuz etkileme ve yaşam kaybına neden olma ve ulusal kritik altyapı yapılarının faaliyetlerini olumsuz yönde etkileme yeteneği"

Amerika Birleşik Devletleri Bilgisayar Acil Durum Hazırlık Ekibi'ni de içeren Amerika Birleşik Devletleri Ulusal Siber Güvenlik Kariyer ve Çalışmaları Girişimi (NICCS), sözlüğünde siber güvenliği şu şekilde tanımlamaktadır:

"Bilgi ve iletişim sistemlerinin ve bunların içerdiği bilgilerin hasar, yetkisiz kullanım veya değişiklik veya istismara karşı korunduğu ve/veya savunulduğu faaliyet veya süreç, yetenek veya yetenek "

Tüm bu tanımların ortak noktası, referans nesnelerinin devletler ya da bireyler olmadıklarıdır. Referans nesneleri bilgisayar sistemleri, veri bütünlüğüne duyulan güven ve ulusal kritik altyapıların, kolektif politikaların ve teknolojilerin sürekli çalışabilirliğidir. Bu da, caydırıcılık veya karşılıklı olarak güvence altına alınmış yıkım gibi eski teorileri benzer şekilde aynı amaca hizmet edecek şekilde

uyarlama olasılığını ortadan kaldırır. Vaka çalışmalarının gösterdiği gibi, siber silah geliştirme maliyetleri, diğer dört alanın geleneksel silahlarının maliyetlerini aşıyor. Ve şimdiye kadar, sadece bir siber silah aslında siber savaş ve hatta siber saldırı tanımlarına uyuyor, Stuxnet. Siber silahların esneklik, makul inkar edilebilirlik sunduğu ve kan dökülmeden arzu edilen bir sonuca ulaştığı belirtilmelidir.

3.Siber Tehditler

Son yıllarda, "siber saldırı" terimi, siber uzaydaki çoğalmaları nedeniyle neredeyse hizmet reddi saldırıları (DoS) ile eşanlamlı hale geldi. DoS saldırıları küresel olarak ve sıklıkla gerçekleşir, ancak devlet ve devlet dışı aktörlerin yanı sıra siber uzaydaki bireyler için ortaya çıkan en büyük tehdit değildir. Projenin ana hedefleri doğrultusunda, bu bölüm siber güvenlik tehditlerini ve bunların devlet ve devlet dışı aktörlere yönelik önemini açıklamayı ve teknik olarak bilgilendirici ve açık kalmayı amaçlamaktadır.

Siber tehditler iki özel kategoride kategorize edilebilir. Hedefli ve hedefsiz siber saldırılar. Aditya K.'ya göre Sood ve Richard Enbody, hedefli siber saldırılar "belirli bir kullanıcıyı, şirketi veya kuruluşu hedefleyen özel saldırılar" olarak tanımlanmaktadır.
kritik verilere gizli bir şekilde erişim" (Sood and Enbody, 2014, s. 2). Hedefli saldırıların tam tersini türeten hedefsiz saldırılar, mümkün olduğunca çok sayıda bilgisayar sistemini/ağını etkilemek amacıyla gerçekleştirilen ayrımcı olmayan saldırılar olarak tanımlanabilir. Hedefli siber saldırılar, doğaları gereği, c yberspace'de, hedeflenmemiş güvenlik açığı arayan ve istismar eden saldırılara kıyasla çok fazla çoğalmamaktadır. Siber uzayın multidisipliner doğası nedeniyle, hem hedefli hem de hedefsiz siber saldırıların siber uzayda ortaya çıkardığı güvenlik zorluklarını daha iyi anlamak için devlete ve Devlet dışı aktörlerin, bu tür saldırıları tanımlayabilmesi ve ayırt edebilmesi gerekir.

3.1 Hedefli Siber Saldırı Vektörleri

Sood ve Enbody, "Hedefli Siber Saldırılar" başlıklı çalışmalarında, hedeflenen siber saldırı vektörlerinin önemli karakter eylemlerinden bazılarını tanımlamaktadır. Tanımlarında, hedefli bir siber saldırı, sıfır gün istismarlarını ve daha önce bilinmeyen güvenlik açıklarını kullanarak kendini gizlemeye çalışırken, mevcut güvenlik yazılımlarından kaçınmak ve saldırganın kimliğini gizlemek için özel olarak yazılmıştır ve yalnızca belirtilen hedeflerin peşinden gitmezken, maruz kalmaktan kaçınmak için düşük değerli hedeflere virüs

bulaştırmak, tüm bunları yaparken söz konusu saldırı operasyonlarını gizlice yürütmek (Sood ve Enbody, 2014, s. 2-3).

3.2 Gelişmiş Kalıcı Tehditler

Hedefli siber saldırılar, "Gelişmiş Kalıcı Tehditler" (APT) etiketli çok daha büyük bir kategorinin bir alt kümesidir. Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü, gelişmiş kalıcı tehditleri şu şekilde tanımlamıştır:

"Birden fazla saldırı vektörü (örneğin, siber, fiziksel ve aldatmaca) kullanarak hedeflerine ulaşmak için fırsatlar yaratmasına izin veren sofistike uzmanlık seviyelerine ve önemli kaynaklara sahip bir düşman . Bu hedefler tipik olarak, bir misyonun, programın veya kuruluşun kritik yönlerini baltalamak veya engellemek amacıyla hedeflenen kuruluşların bilgi teknolojisi altyapısında dayanak noktaları oluşturmayı ve genişletmeyi; veya gelecekte bu hedefleri gerçekleştirmek için kendini konumlandırmak. Gelişmiş kalıcı tehdit: (i) hedeflerini uzun bir süre boyunca tekrar tekrar takip eder ; (ii) savunucuların buna direnme çabalarına uyum sağlar; ve (iii) hedeflerini gerçekleştirmek için gereken etkileşim düzeyini korumaya kararlıdır" (Ulusal Standartlar ve Teknoloji Enstitüsü, 2015, s. B-1).

Hem hedefli siber saldırılar hem de gelişmiş kalıcı tehditler, hedeflerine ulaşmak için yüksek derecede finansman ve teknik uzmanlık gerektirir. However, ikisi de kesinlikle devlet finansmanına ve gözetimine bağımlı değildir. İlk Stuxnet enfeksiyonu, kötü amaçlı yazılımın çalışması için gereken değiştirilmiş sürücü dosyalarını imzalamak için çalıntı dijital sertifikaları kullandığını göstermiştir (Falliere, O Murchu, and Chien, 2011, p. 3). Bu dijital sertifikalar yüksek düzeyde fiziksel güvenlik altında tutulur ve elde etmek için fiziksel erişim gerektirir ve söz konusu sertifikalara sahip şirketlerin fiziksel yakınlığı, Stuxnet'in geliştirilmesinden ve dağıtılmasından sorumlu organizasyon içindeki devlet düzeyinde istihbarat ajanlarını ima eder. Literatür araştırmaları, bazı araştırmacıların tüm APT'lerin devlet destekli kategoriye girdiğini, ancak iyi finanse edilen devlet dışı aktörlerin, özel olarak uyarlanmış kötü amaçlı yazılımlarını gizlemek için Darknet'ten sıfır gün istismarları elde edebileceğini öne sürdüğünü göstermektedir. Darknet'teki sıfır gün istismar fiyatları 1.000 doların altından 100.000 doların üzerine kadar değişmektedir. Stuxnet'in hedeflere nüfuz etmek ve yayılmak için dört sıfır gün istismarı kullandığı ve peer-to-peer (P2P) ağları aracılığıyla kendini güncellediği bilinmektedir (Falliere, O Murchu, and Chien, 2011, p. 2).

APT kampanyaları özellikle hedeflerine yönelik olarak tasarlanır ve net hedeflerle yürütülür. Çok değerli fikri mülkiyetler genellikle bu saldırıların hedefidir. 2013 yılında FireEye raporu, eğitim, finans, yüksek teknoloji endüstrileri, hükümet, danışmanlık firmaları, enerji şirketleri, telekomünikasyonşirketleri, sağlık tesisleri ve havacılık endüstrilerinin APT kampanyaları için ilk on seçenek olduğunu tespit etmiştir (Chen, Desmet, and Huygens, 2014,

s. 64).

Sınıflandırma	Tarih	Sıfırıncı Gün	Hedef
GhostNet	2009 Mart	+	
Aurora	2010 Ocak	+	Yaklaşık 34 ABD şirketi
Stuxnet	2010 Haziran	4 adet	İran nükleer tesisleri
RSA Breach	2011 Ağustos	+.Adobe Flash Player	RSA güvenlik tedbirlerinin kırılması
Duqu	2011Eylül	+ Ms Word True Type Font	Dünya çapında birçek kişisel bilgisayar
Nitro Attack	2011Temmuz	+	Kimyasal ürün üreten şirketler
Taidoor Attack	2011Ekim	9 adet	ABD/TAIWAN GİZLİ BELGELER
Flame (Sky Wiper)	2012 Mayıs	+ Terminal Service	ORTADOĞU ÜLKELERİNDEN SİBER BİLGİ SIZDIRMA

Tablo 3.1, bilinen hedefli siber saldırıların bazılarının yanı sıra gelişmiş kalıcı tehditleri ve bunların hedeflerini güvenlik açıklarıyla birlikte göstermektedir.

3.2.1 Hedefli Siber Saldırıların Aşamaları ve Gelişmiş Kalıcı Tehditler

Sood ve Enbody'ye göre, hedefli siber saldırılar yaşamları boyunca beş farklı operasyon aşamasından geçiyor. Bu beş aşamayı "istihbarat toplama, hedefe virüs bulaştırma, sistem sömürüsü, veri sızıntısı, kontrol ve ağ erişimini sürdürme " olarak tanımlarlar (Sood ve Enbody, 2014, s. 6-8). Karşılaştırmalı olarak, APT'ler kampanyaları sırasında benzer saldırı aşamalarını da paylaşırlar. Chen, Desmet ve Huygens, APT'lerin aşamalarını 6 adımda tanımlar. Keşif ve silahlandırma, yük teslimi, ilk müdahale, komuta ve kontrol, yanal hareket ve son olarak veri sızıntısı (Chen, Desmet ve Huygens, 2014, s. 65). Bu bölüm, hem hedefli siber saldırıların tanımları hem de gelişmiş kalıcı tehditlerin aşamaları arasında paylaşılan ortak noktaları açıklamaya çalışmaktadır.

3.2.1.1 Keşif ve Silahlandırma

"Hedef istihbaratı toplama" olarak da bilinen aşama, bir siber saldırı için bir hedefin keşfedildiği ve seçildiği aşamadır. Hedef hakkındaki bilgiler, Çevrimiçi Sosyal Ağlar (OSN),

kamu hükümet kayıtları veya hedef hakkında ilgili bilgileri tutan web siteleri gibi kaynaklar aracılığıyla toplanır. Bilgi toplama süreci boyunca, saldırgan farklı istihbarat toplama yöntemleri kullanabilir. Açık kaynaklı yazılım tarafından karıştırılmaması gereken Open Source Intelligence (OSINT), erişime açık kaynaklardan istihbarat toplayarak gerçekleştirilir. Siber İstihbarat (CYBINT), veri toplamak için arama motorları veya hedeflerle ilgili zaten tehlikeye atılmış ağlar gibi internet kaynaklarının kullanılmasını ifade eder. Son olarak, İnsan Zekası (HUMINT), hedef hakkında veri toplamak için insan etkileşimini kullanır.

Yeterli veri toplandığında eleme işlemi başlayabilir. Kişisel veya geçmiş veriler, ilişkiler ve kişiler, hedef hakkındaki coğrafi grafik konum gibi ilgili bilgiler kategorize edilebilir ve analiz edilebilir. Verilerin hedefe göre değiştiğini belirtmekte fayda var. Hedefler tek bireylerden büyük kuruluşlara kadar uzanır. Toplanan ve elenen verilerle, kaynak korelasyonu ve bilgi işleme, hedefin ortamını ve davranışlarını tanımlamak ve bunlardan yararlanmak için ilişki verilerini düzenlemeye başlayabilir.

Son olarak, bir saldırı, mızraklı kimlik avı gibi method'lar kullanılarak şimdiye kadar toplanan bilgilerle modellenir ve ilişkilendirilir (Sood and Enbody, 2014, pp. 11-16).

3.2.1.2 Yük Teslimi

İstihbarat toplama işleminin ardından, saldırgan hedefin ağına ait sistemlerden yararlanmak üzere Uzaktan Erişim Araçları'nı (RAT) yüklemek için hedefine virüs bulaştırma işlemine başlar. Bir saldırgan, hedeflerine ulaşmak için iki farklı saldırı türü kullanabilir; doğrudan ve dolaylı saldırılar.

Doğrudan saldırılar, kritik sistemlere erişmek veya hangi dolaylı saldırının daha başarılı olacağını belirleyerek dolaylı saldırıların önünü açmak için istihbarat toplama aşamasında keşfedilen hedef network güvenlik açıklarından yararlanmaya çalışır. Hedef ağın web güvenlik açıklarının karşılaştırmalı analizi. *Dolaylı saldırılar*, kötü amaçlı ekler/bağlantılar içeren sosyal mühendislik veya kimlik avı e-postaları gibi bileşenleri kullanan veya bireylerin tarama alışkanlıklarını patlatarak kritik sistemlere ve ağlara erişmek için su birikintisi yapan katmanlı saldırılardır (Sood and Enbody, 2014, s. 23-24).

Virüs bulaşma aşamasında, bir saldırgan sosyal mühendislik, kimlik avı e-postaları, güvenlik açığından yararlanmanın yanı sıra su birikintisi, otomatik istismar çerçeveleri ve rootkit'ler gibi gelişmiş kötü amaçlı yazılımlar gibi kritik sistemlere erişmek için çeşitli saldırı modelleri kullanabilir.

Sosyal mühendislik, insanın zayıflamışesses'ini, yani saflığı ve cehaletini kullanan bir saldırı yöntemidir. Bir saldırgan, hedefleri kendi güvenliklerini ihlal etmeleri veya ağları hakkındaki hassas bilgileri açığa çıkarmaları için kandırabilir (Smith, Papadaki, and Furnell,

2013, p. 249).

Spear Phishing, yalnızca belirli bir alıcı grubunu, hedeflerin başarı şansını artırmak için gizlenmiş ve kişiselleştirilmiş kötü amaçlı bağlantılar veya ekler içeren sahte e-postalarla hedefleyen bir saldırı modelini ifade eder (Chen, Desmet ve Huygens, 2014, s. 66). Arabayla indirme saldırısı olarak da adlandırılan saldırıda, kullanıcılar, genellikle saldırgan tarafından gönderilen e-postalara gömülü bağlantılar aracılığıyla saldırgan tarafından işletilen kısa ömürlü kötü amaçlı etki alanlarını ziyaret etmeye zorlanır (Sood ve Enbody, 2014, s. 27).

Sulama Deliği / su birikintisi saldırıları, internet kullanıcıları için tarama alışkanlıklarına göre ortaya konan tuzaklardır. Bir saldırgan, saldırganın sık ziyaret ettiği bir üçüncü taraf web sayfasını ele geçirir hedeflerine yönelik bir yük sunmak için söz konusu sayfayı hedefler ve enfekte eder (Sood ve Enbody, 2014, s. 30).

Bir saldırgan, zaten virüs bulaşmış ve hedefin tesislerine teslim edilmiş çıkarılabilir flash sürücüler gibi Evrensel Seri Yol (USB) aygıtlarıyla daha doğrudan yük teslim yaklaşımı kullanabilir. Bir çalışan, bu sürücülerden birini tesisin etrafında yerleştirebilir ve sahibini bulmak ve iade etmek amacıyla bilgisayarlarına takabilir. Bununla birlikte, çoğu bilgisayar sistemi, takıldıktan sonra bir flash sürücünün içeriğini otomatik olarak yürütecek şekilde ayarlanmıştır. Bu noktada, yük zaten teslim edilir ve enfeksiyon aşaması başarılı olur (Sood ve Enbody, 2014, s. 32).

3.2.1.3 İlk İzinsiz Giriş ve Sistem İstismarı

Yük tesliminin ardından, bu aşamada bir saldırgan hedefin ağına başarıyla sızar. Genellikle, kampanyanın bu aşamasında iki tür istismar başlatma rampaları kullanılır : Tarayıcı tabanlı açıklardan yararlanma girişimleri ve belge tabanlı açıklardan yararlanma girişimleri. Tarayıcı tabanlı açıklardan yararlanma girişimleri Internet Explorer gibi tarayıcılarda bulunan güvenlik açıklarından yararlanmaya çalışırken, belge tabanlı açıklardan yararlanma girişimleri ise Uzaktan Erişim Araçları'nı (RAT) Internet Explorer gibi tarayıcılarda bulunan güvenlik açıklarından yararlanmaya çalışır erişimi sürdürmek için hedef bilgisayar (Chen, Desmet, and Huygens, 2014, p. 67).

Tarayıcı Açıklardan Yararlanma Paketleri, tarayıcılarda bulunan üçüncü taraf yazılımlar da dahil olmak üzere tarayıcı yazılım ortamlarındaki bilinen ve bilinmeyen (sıfır gün) güvenlik açıkları için açıklardan yararlanma durumlarını bir araya getiren bir yazılım çözümüdür. Manuel giriş gerektirmeden tamamen otomatik olan BEP'ler, ilk izinsiz giriş sürecini otomatikleştirerek saldırganların iş hayatını azaltır (Sood ve Enbody, 2014, s. 40).

Sıfır gün güvenlik açığı, şu anda bilinmeyen ve bu nedenle yazılım geliştiricileri tarafından yamalanmamış olarak kalan bir güvenlik açığıdır. Başarılı bir uzaktan yürütülebilir dosyanın güvenlik açığı penceresine bağlı olarak, sıfır gün istismarları, bir saldırganın bilinen güvenlik

açıklarına dayanarak zaten kurulmuş bir siber savunma çevresini atlatması için büyük bir avantaj sağlayabilir. Güvenlik açığı keşfedilse ve daha sonra p eklense bile, kesinti süresinin genellikle kabul edilemez olduğu sürekli çalışan sistemler söz konusu olduğunda, yamaların yayılma penceresi aylar veya yıllar sürebilir. Bu nedenle, sıfır gün güvenlik açıkları bulunup yamalansa bile, some sistemlerinde hala mevcuttur ve ilk gün için hala geçerli saldırı vektörleridir.

3.2.1.4 Komuta ve Kontrol

Kampanyanın bu aşamasında, saldırganlar meşru çevrimiçi hizmetlerden halka açık araç setlerine ve ticari istismar araçlarına kadar çeşitli araçlar kullanarak ağdan daha fazla yararlanmak için komuta ve kontrol tekniklerini kullanır. Bir saldırgan, kötü amaçlı yazılımlarını güncelleştirmeler veya blog gönderileri aracılığıyla OSN'lere kayıtlı bir hesaptan komut arayacak şekilde programlayabilir; hem saldırganın hem de izinsiz girişin kara listeye alınmasını veya tanımlanmasını önlemek için TOR anonimlik ağları üzerinden gelen bağlantıları yapılandırmak; sunucu-istemci parametreleriyle çalışan meşru veya başka bir şekilde uzaktan erişim araçlarını dağıtın. Bu kategorilerle sınırlı olmamakla birlikte, çoğu APT kampanyasının komuta ve kontrol aşamaları, kampanyayı bir sonraki aşamaya taşımak için bu sloganlar etrafında döner (Chen, Desmet, and Huygens, 2014, p. 67). Algılamadan kaçınmak, komuta ve kontrol sunucuları genellikle üç ayrı kategoride kategorize edilir: Merkezileştirilmiş, merkezi olmayan ve hibrit komuta ve kontrol servers.

Merkezi komuta ve kontrol sunucuları kavramı, kötü amaçlı yazılımların tek bir sunucu varlığı tarafından kontrol edildiği anlamına gelir. Bu, kötü amaçlı yazılımı, Stuxnet solucanında olduğu gibi keşif üzerine DNS kara listesine karşı savunmasız bırakır. DNS kara listesini azaltmak için tasarlanan *merkezi olmayan komut ve fetih sunucuları*, kötü amaçlı yazılımın her örneğini P2P bağlantıları üzerinden bir komut aktarma mekanizması olarak kullanır. Son olarak, *hibrit komuta ve kontrol sunucuları* her iki dünyanın da en iyisine sahip olacak şekilde tasarlanmıştır. Birincil kontrol yönteminin ana sunucuya geri bağlantı kuramaması durumunda her iki yöntemi de geri dönüş mekanizması olarak kullanırlar (Sood ve Enbody, 2014, s. 87).

3.2.1.5 Yanal Harekât

Operasyonun bu aşamasında saldırganlar "dahili performans göstererek" değerli verileri bulmak ve çıkarmak için ihlal edilen ağ içindeki saldırılarını genişletirler ve ağın haritasını çıkarmak ve istihbarat elde etmek için keşif ; kimlik bilgilerini toplamak için ek sistemlerden ödün vermek ve de yükseltilmiş ayrıcalıklar kazanmak; kalkınma planları veya ticari sırlar gibi değerli dijital varlıkların tanımlanması ve toplanması" (Chen, Desmet, and Huygens, 2014, p. 68).

3.2.1.6 Veri Sızıntısı

Hedef veriler saldırganlar tarafından bulunup ele geçirildikten sonra, bu verilerin sızdırılması kampanyadaki son adım haline gelir. Kötü amaçlı yazılımın saldırgan tarafından nasıl tasarlandığına bağlı olarak, sızma için işaretlenmiş veriler, komuta ve kontrol sunucularına geri dönmek için farklı yöntemler seçebilir. Son kötü amaçlı yazılım aileleri, kuruluşların güvenliğini sağlayan çoğu güvenlik duvarı HTTP verilerinin geçmesine izin verdiğinden, verileri sızdırmak için Köprü Metni Aktarım Protokolü (HTTP) ve Güvenli Köprü Metni Aktarım Protokolü (HTTPS) protokollerini tercih etmektedir. HTTPS ayrıca içeriğin şifrelenmesine izin verir ve son kullanıcıların sistemleri tarafından oluşturulan söz konusu paketleri analiz etmek için derin paket inceleme yöntemi olmadan, BT yöneticileri içeriği keşfedemez. Veri sızdırma teknikleri HTTP protokolleriyle sınırlı değildir, Dosya Aktarım Protokolü (FTP), P2P bağlantıları, Secure Shell (SSH) protokolü, Basit Posta Aktarım Protokolü (SMTP) gibi alternatif protokoller ve hatta DNS sorguları programlanabilir. Şifrelenmiş verileri iletmek. Bununla birlikte, FTP, SSH, SMTP protokolleri genellikle en çok saniyelik bir ortamda izlenir, bu da HTTP'nin son kötü amaçlı yazılım ailelerinde ana veri sızıntısı seçeneği olarak popülaritesinin artmasını açıklar (Sood and Enbody, 2014, pp. 86-90).

3.2.2 Hedefli Siber Saldırılara Karşı Önlemler

3.2.2.1 Güvenliğe Üç Yaklaşım

Gelişmiş kalıcı tehditler, hem BT yöneticileri tarafından kaçırılması kolay maliyetli saldırılardır hem de güvenli ağ içindeki saldırganlar tarafından bir dayanak noktası oluşturulduktan sonra ortadan kaldırılması zordur. Birçok saldırı yöntemi ve saldırı noktası, APT'lerin her şeyi yakalayan önlemlerle çözülemeyeceği veya sadece özenle hareket eden BT uzmanları tarafından durdurulamayacağı anlamına gelir. Sood ve Enbody, hedeflenen siber saldırılara karşı önlemleri üç kategoride sınıflandırır: kullanıcı merkezli çalışma, son sistem güvenliği, ağ düzeyinde güvenlik(Sood ve Enbody, 2014, s. 128-130).

"Kullanıcı merkezli güvenlik", son sistemleri işleten kullanıcıların, hedeflenen siber saldırıların yanı sıra gelişmiş kalıcı tehditlerin yarattığı tehditlerden haberdar edilmesi gerektiği anlamına gelir. Eğitim yoluyla güvenli ağ ortamlarında kullanıcı davranışını iyileştirmek için belirli yöntemler vardır. Güvenli bilgi işlem uygulamalarının kullanıcılara delinmesi ve düzenli aralıklarla değiştirilen daha güçlü benzersiz parolalar kullanmaları istenmesi gerekir. Mümkünse, kullanıcıların tarama ihtiyaçları için sanal makineler (VM) kullanmaları teşvik edilmelidir, böylece drive-by saldırıları ana bilgisayar sisteminin güvenliğini tehlikeye atamaz. Ayrıca, genellikle sofistike kötü amaçlı yazılımların güvenlik

uzmanları tarafından analiz edilmekten kaçınmaya çalıştığını ve bu nedenle sanal bir ortamda sınırlandırıldığında farklı tepki vereceğini belirtmek gerekir. Kimlik avı yoluyla bilgi kaybını önlemek için kullanıcılara bilgi güvenliği standartları aşılanmalıdır. Kötü amaçlı kodların ağı ihlal etmesini önlemek için kullanıcıların güvenli ağ içinde kendi USB cihazlarını kullanmaları engellenmelidir (Sood ve Enbody, 2014, s. 129).

Kullanıcıları APT'nin tehlikeleri ve maliyetleri hakkında eğitmek, son sistem güvenlik önlemlerine sahip güncel bilgisayar sistemleriyle iltifat edilmelidir. İşletim sistemlerinin, üçüncü taraf uygulamaların, ilgili en son sürümlerine yamalanması gerekir. Yukarıda belirtildiği gibi, tarama amacıyla, ana bilgisayarı arabayla indirmelerden ve kötü amaçlı web sitelerinden korumak için sanal makineler kullanılmalıdır. Bu adımlar atılsa bile, güvenlik açıklarından yararlanan bilinen kötü amaçlı yazılımlara karşı koruma sağlamak için bir anti-virüs bu nedenle ftware dağıtılmalıdır (Sood and Enbody, 2014, s. 128).

Son olarak, ağ düzeyinde güvenlik, saldırı tespit sistemleri (IDS) ve izinsiz giriş koruma sistemleri (IPS) gibi ağ düzeyinde güvenlik araçlarının ve uygun şekilde kullanılmasını ifade eder. bilinen kötü amaçlı yazılım komutunun ve kontrol sunucularının DNS istekleri tarafından çözümlenmesini engellemek ve anormal ağ tr affic'i tespit etmek ve sonlandırmak için ağ trafiğini izlemek üzere yapılandırılmış güvenlik duvarları. SSL teknolojisini kullanarak veri akışına yönelik ortadaki adam (MitM) saldırılarını önlemek için hassas verilerin doğru şekilde şifrelenmesinin yanı sıra ağ yöneticileri tarafından yapılan özenli sunucu ve güvenlik duvarı günlükleri okuması, veri kaybını ve kötü amaçlı kod yayılımını azaltmaya yardımcı olur. Son olarak, ağlar ve kullanıcılar, APT'lerin yanal hareketlerine ve katran kaynaklı siber saldırılara karşı sertleşmek için uygun şekilde sabitlenmiş ve muhafazaedilmiş yazıcılar, yönlendiriciler, erişim noktaları gibi ağa bağlı cihazlarla sanal yerel alan ağları (VLAN) içinde ayrılmalıdır (Sood and Enbody, 2014, pp. 129-131).

Tablo 3.2, APT saldırısının her aşamasında saldırı yöntemlerini önleyici önlemlerle karşılaştırmaktadır.

Stage	Attack Method	Countermeasure
Reconnaissance and Weaponization	OSINT, Social engineering, Malware preperation,	Security awareness training, Patch management, Firewall
Delivery	Spear Phishing, Watering hole attack	Content filtering software, NIDS, Anti-virus software
Initial Intrusion	Zero-day exploits, Remote code execution	Patch management, HIDS, Advanced malware detection
Command and Control	Exploiting legitimate services, RAT, encryption	NIDS, SIEM, Event Anomaly detection
Lateral Movement	Privilege Escalation, Collecting data	Access Control, HIDS, NIDS, Event Anomaly detection
Data Exfiltration	Compression, Encryption, Intermediary Staging	Data Loss Prevention

3.2.2.2 *Açık Kaynak ve Özel Yazılım Karşılaştırması*

Önceki bölümlerde daha önce de belirtildiği gibi, sıfır gün güvenlik açıkları, şu anda siber alanda güvenliği tehdit eden en yaygın olarak kullanılan güvenlik açıklarından biridir. Bununla birlikte, bunun nedeni, yazılımın geliştirme ve yayınlama döngüleriyle mümkün olduğunca verimli bir şekilde başa çıkmaya çalışan ve güvenlik açıkları bırakan sınırlı sayıda yazılım geliştiricisinden kaynaklanmaktadır. Sıfır gün güvenlik açığına yönelik bir yamanın tüm kullanıcılara dağıtılması bir yıl kadar sürebilir. Dünya çapındaki bilgisayarların çoğunu savunmasız bırakıyor. Kritik altyapılar, mümkün olduğunca fazla kesinti süresiyle çalışması gereken sistemlerdir. Günümüzün modern dünyasında, tüm teknolojik cihazlar bir tür mülkiyet veya açık kaynaklı yazılım üzerinde çalışır. Bazen ikisi de aynı anda. Güvenlik bilincine sahip bir bakış açısıyla karşılaştırmadan önce iki tür yazılım türünü tanımlamak faydalı olacaktır. *Açık* kaynaklı yazılım (OSS) terimi, Linux topluluğu içinde tanınmış bir açık kaynaklı kurumsal yazılım çözümleri şirketi olan RedHat'in sahip olduğu ve işlettiği bir web sitesi olan opensource.com tarafından "kaynaklı yazılım" olarak tanımlanmaktadır.

Öte yandan, açık kaynaklı yazılım, daha hızlı yama dağıtım fırsatları nedeniyle daha hızlı keşif, daha iyi güvenlik açığı koruması sağlar, ancak kaynak kodunu okuma, değiştirme ve yeniden derleme yeteneği insan kaynaklarını gerektirdiğinden, çok daha fazla bilgisayar sistemi bilgisi gerektirir. Stuxnet'in vaka çalışmasında daha ayrıntılı olarak açıklanmak üzere, programlanabilir mantık denetleyicisi ile Microsoft Windows işletim sistemini çalıştıran ana bilgisayar bileşeni arasındaki veri senkronizasyonundan sorumlu Siemens Step 7 yazılımının yalnızca tek bir bileşeni hedeflenmiştir.

3.3 Hedefsiz Siber Saldırılar

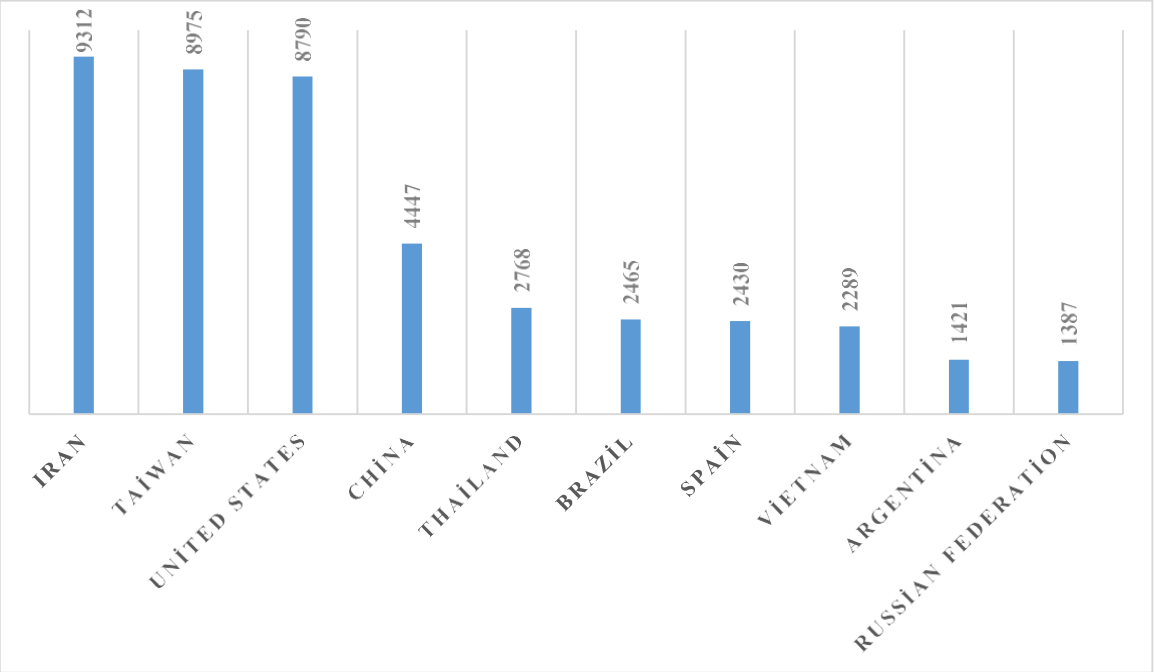
Hedefli siber saldırıların aksine, hedefsiz siber saldırılar hedefler arasında ayrım yapmaz. Bu saldırılar genellikle kendilerini geniş bir ağ olan casting aracılığıyla gösterir. Bu saldırı türleri, devletlerin siber uzaydaki varlığına hala zararlı olsa da, devlet dışı aktörlere, yani bireylere ve işletmelere karşı en etkili olanlardır.

3.3.1 Hizmet Reddi

Hizmet Reddi saldırıları, siber uzaydaki tek varlıklara, örneğin tek bir web sitesine karşı gerçekleştirilebilir veya sırasıyla Estonya ve Gürcistan siber saldırıları durumunda, 2007 ve 2008 siber saldırıları, ayrım gözetmeksizin bir ülkeye ait ağlara karşı başlatılabilir. Dağıtılmış Hizmet Reddi saldırıları, bir ağın ve kullanıcılarının ayrılması olan amacını gerçekleştirmek ve gerçekleştirmek için birkaç başka bileşen daha gerektirir. Bir saldırının nasıl taşındığını anlamak için, bu bileşenlerden bazılarının açıklanması gerekir. DDoS saldırıları genellikle insan bilgisayar etkileşimi katmanı olan birbirine bağlı hesaplamanın OSI Modelinin yedinci katmanında üretilir (Uluslararası Telekomünikasyon Birliği, 1994, s. 33).

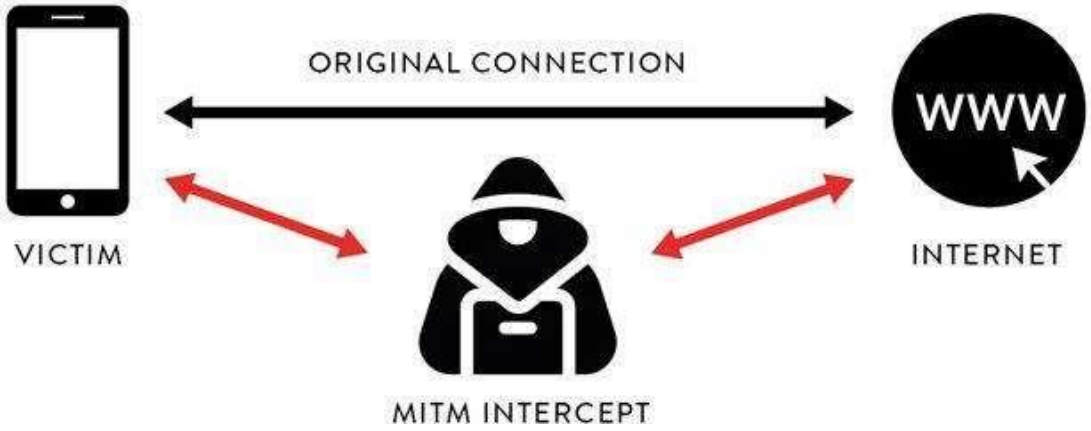
Tipik bir saldırı senaryosunda, saldırgan interneti tarayarak güvenlik açığından etkilenen bilgisayarları ele geçirip bot ağlarına ekler. Saldırgan tarafından enfekte olan savunmasız bir bilgisayar daha sonra "yanal hareket" olarak adlandırılan şey aracılığıyla kendi iç ağındaki diğer aygıtları arar ve bulaştırmaya çalışır. Önemlisayıda virüslü cihaz saldırgan tarafından kontrol ediliyorsa, saldırgan hizmet reddi saldırısını başlatabilir . Dağıtılmış hizmet reddi saldırısı, yüksek trafik oluşturma yükünün saldırganın botnet'ine ait bilgisayarlar arasında, botlara hedefe mümkün olduğunca çok HTTP isteği göndermeleri talimatı verilerek dağıtıldığı anlamına gelir. kısa bir süre, böylece hedefin meşru isteklere yanıt verme kapasitesini kısıtlar. Bu da, hem Tallinn (2007) hem de Georgia (2008) siber saldırılarında olduğu gibi, etkilenen ağlar için hizmet kesintilerine yol açmaktadır.

Şekil 3.1 Varsayılan parola ile kullanılan internete bağlı cihaz sayıları



3.3.2 Ortadaki Adam Saldırıları

Ortadaki Adam (MiTM) saldırıları, bir saldırgan iki varlık arasındaki iletişimi kestiğinde gerçekleşir . Bu tür bir saldırı siber uzaydan önce de vardı ve hem gerçek dünyada hem de cyberspac e'de hala geçerli. Gerçek dünya senaryosunda, saldırgan bir alıcının postasını teslim edilmeden önce veya aktarım sırasında ele geçirerek içeriğini değiştirebilir. Siber uzayda, yazılım otomasyonu sayesinde MiTM saldırıları daha kolay gerçekleştirilir. Diğer saldırı vektörlerinin aksine, MiTM saldırıları sadece gerekli güvenlik yamalarıyla güncel kalarak önlenemez. MiTM saldırıları çeşitli vektörler aracılığıyla gerçekleştirilebilir. Stacy Prowell, Rob Kraus, Mike Borkin, "Yedi En Ölümcül Ağ Saldırısı" başlıklı çalışmalarında, bir kullanıcı ile bir sunucu arasındaki veri paketlerini ele geçirme hedefine ulaşmanın dört farklı yolunu bildirmektedir: Ağ trafiğini koklama, yeniden yürütme saldırıları, komut ekleme ve son olarak Internet Control Message Protocol (ICMP) yeniden yönlendirmesi (Prowell, Kraus, and Borkin, 2010, pp. 104-105).



Şekil 3.2 Ortadaki Adam Saldırılarının bir tasviri

3.3.3 Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılımlar veya sadece kötü amaçlı yazılımlar, sistem yazılımının operatörünün izni olmadan kötü amaçlı görevleri yerine getirmek için yazılmış yazılımlardır. Genellikle hedefli saldırılardan ziyade kitlesel enfeksiyon için oluşturulan bu programlar, belirli kullanımlar için uyarlanmıştır. Bu bölümde, bu kötü amaçlı yazılımların bazı işlevleri kısaca açıklanmaya çalışılmaktadır.

3.3.3.1 Virüs

Virüsler, kendisini diğer yürütülebilir dosyalara enjekte edebilen ve ho sting yürütülebilir dosyalarıyla birlikte yürütülen bilgisayar kodlarıdır. Virüs, sisteme veya önyükleme işlemi yürütülebilir dosyalarına bulaşabilir ve bilgisayarın çalıştığı süre boyunca Rastgele Erişim Belleğinde (RAM) kalabilir, bundan böyle çalışma süresi olarak anılacaktır. Yerleşik virüs daha sonra yayılma girişiminde bulunarak kendisini diğer yürütülebilir dosyalara bulaştırabilir ve çoğaltabilir (Abraham, 2018).

3.3.3.2 Solucan

Bilgisayar solucanları kendi başlarına programlardır ve ortak hizmetlerdeki güvenlik veya ilke güvenlik açıklarından yararlanan bir ağa yayılırlar. Diğer yürütülebilir dosyaları enfekte etmedikleri için virüslerden farklıdırlar, bu nedenle alternatif ancak daha hızlı yayılma yöntemlerine sahiptirler (Weaver, Paxson, Staniford, and Cunningham, 2003, p. 1). Solucanlar ve virüsler genellikle e-posta ekleri yoluyla ve already virüslü bir USB sürücü takılarak yayılır.

virüs tarafından virüs bulaşma protokolünü otomatik olarak yürütmek üzere programlanmış bir bilgisayara. Kötü şöhretli Stuxnet kötü amaçlı yazılımının bir solucan olarak sınıflandırıldığını ve bu çalışmada böyle adlandırılacağını belirtmekte fayda var.

3.3.3.3 Trojan

Adını Truva Savaşı'nda Truva'ya hediye edilen ünlü tahta attan alan Truva atı, "[programı çalıştıran] kullanıcının ayrıcalıklarından kaynaklanan bir güvenlik tehdidiyle yararlanabilen gizli işlevler içeren, görünüşte yararlı bir programdır" (Ford, 1999, s. 105). Virüslerin veya solucanların aksine, truva atları kendi başlarına yayılmaz. Çoğu zaman, Truva atlarının tahta atı şehir surlarının içine soktuğu gibi, kullanıcıların bunları güvenli ağlarında isteyerek indirmelerine ve yürütmelerine güvenirler.

3.3.3.4 *Casus Yazılımlar*

Casus yazılımlar, ana bilgisayara doğrudan zarar vermek yerine kullanıcının eylemlerini izleyerek bulaştığı sistem hakkında bilgi toplamak için tasarlanmıştır. Raporlama yetenekleri basit web kullanımı izlemeden tuş kaydetme ve dosya incelemesine kadar uzanmaktadır (Baskin, et al., 2006, p. 2). Duqu kötü amaçlı yazılımı, saldırganların virüslü bilgisayarlarda casusluk yapmasını sağlayan bileşenlere sahip olabilir, ustalarına uzaktan yetenekler verdiği ve bu nedenle uzaktan erişim aracı olarak sınıflandırıldığı için kapsamın dışında basit bir casus yazılımdı

3.3.3.5 Botnet

DoS saldırılarında daha önce bahsedilen bot kötü amaçlı yazılımları, büyük miktarda bilgisayar sistemine virüs bulaştırmak ve kontrol altına almak ve operatörüne uzaktan kontrol yeteneği sağlamak için tasarlanmıştır. Virüsler veya truva atları yoluyla ilk bulaşmadan sonra, virüslü ana bilgisayarı DDoS saldırılarında söz konusu bilgisayar sistemlerini kullanabilecek veya spam / kimlik avı e-postaları gönderebilecek uzak operatöre devretmek için bir bot kötü amaçlı yazılımı indirilebilir. (Lysne, 2018, s. 58).

2011 yılında Festi adlı bir botnet, Rusya'nın en büyük havayolu şirketi olan Aeroflot ile sözleşme görüşmeleri yapan Assist adlı bir ödeme işlemcisine karşı DDoS saldırısı başlatmak için kullanıldı. Saldırı, Aeroflot'un nihai kararından sadece bir hafta önce başlatıldı.

3.3.3.6 Rootkitler

Rootkit'ler, başka bir kötü amaçlı yazılımın varlığını kullanıcı veya kötü amaçlı yazılımdan koruma programları tarafından algılanmaktan gizlemek için kullanılır. Tipik

olarak, rootkit'ler bir bilgisayar sistemine zarar vermez, ancak diğer kötü amaçlı yazılımları gizleme yetenekleri nedeniyle, karmaşık saldırılarda yaygın olarak kullanılırlar (Lysne, 2018, s. 58-59).

3.3.3.7 Fidye Yazılımı

Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) tarafından istihdam edilen Bilgisayar Acil Durum Hazırlık Ekipleri (CERT), veri kaybıyla mücadele için 3, 2, 1, yedekleme sistemi önermektedir. 2 farklı ortamda tutulan herhangi bir önemli dosyanın 3 ayrı kopyası, örneğin bir kopyanın bir hard drive'da tutulması gibi . diğeri kompakt bir disk gibi sadece ortamı okumak için yakılır ; 1 kopya tesis dışında saklanır (Ruggiero ve Heckathorn, 2012, s. 1). Veri depolama teknolojilerindeki son gelişmeler, kompakt diski veri depolama için bir ortam olarak geçersiz kıldı. Bunun yerine, bulut depolama artık her zamankinden daha erişilebilir. Bulut depolamanın salt okunur bir ortam olmadığını ve internette olmanın kopyayı diğer siber tehditlere karşı savunmasız bıraktığını belirtmek gerekir.

Ransomware saldırıları beş aşamada gerçekleştirilir.

Fidye yazılımı kötü amaçlı yazılımlarının ilk dağıtımı, güvenliği ihlal edilmiş web siteleri, drive-by indirmeleri veya kötü amaçlı bağlantılar/ekler içeren kimlik avı e-postaları aracılığıyla başlar ve yayılır. Kötü amaçlı yazılım indiricisi bir sisteme bulaştığında, fidye yazılımı saldırısı kurulum aşamasına girer. Genellikle fidye yazılımları, anti-virüs yazılımı tarafından algılanmasını önlemek için hedef sisteme ilk müdahaleden sonra yeniden monte edilir. Bu noktada fidye yazılımı, sızılan ağ üzerinde yanal olarak hareket etmek için güvenlik açıklarından ve dosya paylaşımlarından yararlanmaya çalışır. Fidye potansiyelini en üst düzeye çıkarmak. Yeniden yapılandırılmış ve komutları bekleyen fidye yazılımı, komut ve kontrol sunucularına bağlanmaya çalışır. Bir bağlantı kurulduktan sonra, kötü amaçlı yazılımlar şifreleme için kişisel belgeler veya resimler gibi potansiyel dosyaları tanımlamak ve daha fazla tırmanma için hedefe sızdı. Hedef dosyalar seçildikten sonra, gelişmiş fidye yazılımları genellikle benzersiz şifreleme anahtarları oluşturur ve bunları komut ve kontrol sunucularına gönderir. Virüslü bilgisayardaki veya ağdaki verileri şifrelemek için komut ve kontrol sunucuları tarafından bir emir döndürülürse, dördüncü saldırı aşaması başlar. Yok etme aşamasında, önceden tanımlanmış önemli dosyalar, son aşamada oluşturulan benzersiz anahtarla şifrelenir. Fidye yazılımı saldırısının son aşamasında, kurbanlar kripto para birimlerinde veya ön ödemeli kartlarda belirli miktarda mone y ödemelerini söyleyen bir ekranla karşılanıyor. Uyumsuzluk durumunda, genellikle fiyat artar veya dosyalar kalıcı olarak silinir (Liska ve Gallo, 2017, s. 6-11).

Gerçek hayatta yaşanan gasp vakaları gibi, uyumluluk da fidye yazılımı saldırılarında

verilerin güvenli bir şekilde geri dönmesini garanti etmez. Basitçe bu nedenle, bu bölümün başındaki veri yedekleme önerisine uygun olarak oluşturulan yedeklemelerden veri kurtarma, verilerin güvenli bir şekilde geri dönmesini garanti etmenin tek yolu olacaktır.

Stage	Actions
Deployment	Compromised web sites
	Drive-by downloads
	Phishing
	Vulnerability Exploitation
Installation	Reconstruction
	Memory Access
	Lateral Movement
Command and Control	HTTP/HTTPS connection
	OSN Instructions
	TOR
	Email
Destruction	Data Encryption
	System Locking
Extortion	Cryptocurrencies
	Prepaid Vouchers

Tablo 3.3 Fidye Yazılım İşletme Süreçleri

4.Örnek Olay İncelemeleri

Projenin bu bölümü, şüpheli failler veya hedefler olarak devlet aktörlerini içeren yüksek profilli siber saldırıların bazılarına odaklanmaktadır.

4.1 Hedefli Siber Saldırılar

4.1.1 Olimpiyat Oyunları Operasyonu (Stuxnet)

Stuxnet, bünyesinde taşıdığı birkaç özellik nedeniyle emsal teşkil etmektedir. Stuxnet kampanyasının ilk keşif ve tanımlama sürecinde, Amerika Birleşik Devletleri (ABD) ve İsrail olmak üzere birkaç devlet aktörünün olaya karıştığından şüphelenildi. 2016 yılında Alex Gibney, "Zero Days" adlı belgeselinde şunları iddia etmişti:

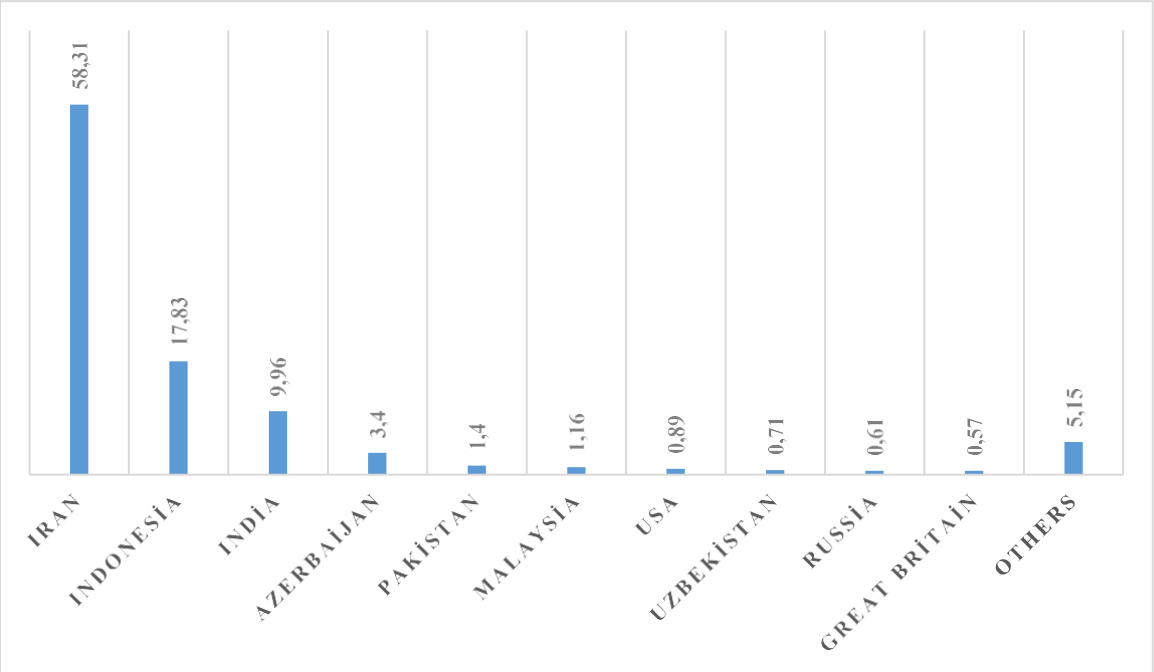
Stuxnet, ABD Ulusal Güvenlik Ajansı (NSA) ile İsrail'in Olimpiyat Oyunları Operasyonu olarak adlandırılan 8200 Birimi arasında bir ortak girişimdi. Gibney çalışmasında ayrıca, dönemin

ABD Başkanı Barack Ob ama'nın, siber silahların konuşlandırılmasının nükleer silahlarla aynı şekilde ele alındığı ve bu nedenle başkanlık izni gerektirdiği için Olimpiyat Oyunları Operasyonu için yeşil ışık yaktığını iddia ediyor. Gibney ayrıca, NSA ve Birim 8200 tarafından geliştirildiği iddia edilen siber silaha dayanan 24 Haziran 2012'nin son kullanma tarihinin, yaklaşan başkanlık seçimleri nedeniyle bu tarihe ayarlandığını iddia ediyor. Stuxnet'in devlet aktörü düzeyinde destek gerektiren karmaşıklığı göz önüne alındığında, herhangi bir teminat hasarını önlemek için nasıl programlandığı ve güvenlik analistleri tarafından kurtarılan tüm sürümlerde önceden belirlenmiş bir son kullanma tarihine sahip olması, Stuxnet'e diğerlerine göre öncelik vermektedir.

4.1.1.1 Stuxnet Nedir?

Kaspersky Lab'in kurucu ortağı ve CEO'su Eugene Kaspersky, 2010 yılında Münih'teki Kaspersky Güvenlik Sempozyumu'nda yaptığı konuşmada Stuxnet'in dikkat çekici karmaşıklığına şu sözlerle dikkat çekti : "Bence bu, dönüm noktası, bu gerçekten yeni bir dünyaya geldiğimiz zamandır, çünkü geçmişte sadece siber suçlular vardı, şimdi korkarım ki siber terörizm, siber silahlar ve siber savaşların zamanı geldi.
... Bu kötü amaçlı program para çalmak, spam göndermek veya kişisel verileri ele geçirmek için tasarlanmamıştır. Bu kötü amaçlı yazılım parçası, bitkileri sabote etmek, endüstriyel sistemlere zarar vermek için tasarlandı".

Stuxnet başlangıçta Sergey Ulasen tarafından keşfedildi, daha sonra VirusBlokAda adlı küçük bir Beyaz Rusya şirketi için çalıştı. Stuxnet, ancak İran'daki bilgisayarlar açıklanamayan Mavi Ölüm Ekranları (BSoD) hataları göstermeye başladıktan sonra keşfedildi. Ulasen, ağa[2] bağlı bilgisayarların, işletim sisteminin yeni bir kurulumuyla bile aynı hataları bildirdiğini öğrendiğinde kötü amaçlı yazılım varlığından şüphelenmeye başladı. Sonunda, Ulasen'in çabaları kötü amaçlı yazılımın bulunmasında verimli oldu ve analiz süreci başladı. 17 Haziran 2010'da VirusBlokAda, Stuxnet'i Rootkit.TmpHider olarak bildirdi ve Bunu takiben, kötü amaçlı yazılımlar dünya çapında tespit edildi ve enfeksiyonların çoğu coğrafi olarak İran'da bulunuyordu. Nicolas Falliere, Liam O Murchu ve Eric Chien, raporlarında, kötü amaçlı yazılımın ilk tohumlanmasının İran'ın varlığına sahip beş farklı kuruluşa bulaşarak yapıldığı sonucuna vardılar. Stuxnet'in bilinen en eski sürümü, bu beş kuruluşa zaten virüs bulaşmış bir USB sürücü aracılığıyla virüs bulaştırmak için kullanıldı ve üç kuruluş bir kez saldırıya uğradı ve kalan ikisi üç kez hedef alındı .



Şekil 4.1 Stuxnet virüsünün coğrafi olarak dağılımı

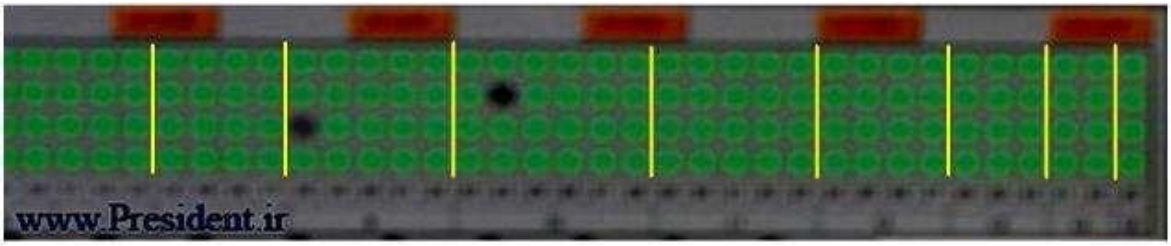
Stuxnet'in güvenlik araştırmacıları tarafından bulunup analiz edildiği noktaya kadar, basit disketlere sığabilecek bir kötü amaçlı yazılım tarafından yapılan kıyamet seviyesi yıkımını öngören bilim kurgu hikayeleri, aktif bir hayal gücünün hikayeleriydi. Ancak Stuxnet, yeterli bilgi ve finansmanla bu hikayelerin sonuçta gerçekleşebileceğinin kanıtıydı. Endüstriyel kontrol sistemlerini hedefleyerek mümkün olanlarla karşılaştırıldığında, Stuxnet'in zararsız bir kötü amaçlı yazılım olarak kabul edildiğini belirtmek gerekir. Siemens Programlanabilir Mantık Denetleyicilerini kontrol eden Siemens'in SIMATIC Step 7 yazılımını çalıştıran yalnızca Microsoft Windows sistemlerini hedefleyen Stuxnet, hedefleri konusunda son derece seçicidir (Falliere, O Murchu, and Chien, 2011, p. 3).

Stuxnet'in operasyonel kampanya sürecinde birkaç önemli farklılığı vardır. Yani, veri sızdırmaya çalışmaz. Bunun yerine, enfeksiyonun son aşamasında, Stuxnet uranyum yakıt zenginleştirme işlemine zarar vermeye çalışır. Çoğu zaman endüstri lkomuta sistemleri doğrudan internete bağlı değildir. Hedefinin doğası gereği Stuxnet, komuta ve kontrol sunucularıyla sürekli iletişim halinde kalamaz. Bu nedenle Stuxnet, bir d raporunu güncel tutmak için Eşler Arası (P2P) bağlantıları kullanır; bu, komuta ve kontrol sistemleri için kullanılan veri paketlerinin, operasyonel bir internet bağlantısına sahip olan aynı ağ içindeki zaten virüslü bir makineye aktarıldığı anlamına gelir (Matrosov A., Rodionov, Harley ve Malcho, 2011, s. 56).

İlk keşif ve silahlandırma aşamasında, saldırganların, kötü amaçlı yazılımların bu

boşluğun üzerinden atlama yollarını simüle etmek ve geliştirmek için hava boşluklu ağlarda olmak gibi aynı konfigürasyondaki santrifüjleri kontrol etmek için gerekli tüm donanımlar da dahil olmak üzere, saldıracakları ayna ortamıyla aynı şekilde kurmaları gerekecektir. Paul Mueller ve Babak Yadegari, "Stuxnet Solucanı" adlı çalışmalarında, çekilen ve basına dağıtılan fotoğraflara dikkat çekiyorlar (İran İslam Cumhuriyeti Cumhurbaşkanı Mahmud Ahmedinejad, Natanz Yakıt Zenginleştirme Tesisi) İran'ın zenginleştirme sürecini detaylandırıyordu (Mueller ve Yadegari, 2012, s. 1). İran, Uranyum-238'i (U 238) Uranyum-235'ten (U^{235}) ayırmak için gaz santrifüjlerini, Uranyum Hekzaflorürü (UF_6) gaz santrifüj tüplerinde yüksek hızlarda döndürerek kullanmıştı. İşlem, silindirin kenarında toplanan daha ağır U 238 atomları ile sonuçlanırken, daha hafif U^{235} atomları ce ntrifuge'un merkezi etrafında kümelenir. Birbirine bağlı gaz santrifüjlerinin bu düzenine kaskad denir.

Şekil 4.2 Dönemin İran Cumhurbaşkanı Mahmud AHMEDİNECAD Natanz'daki tesiste incelemelerde bulunurken



Şekil 4.3 hata durumu oluşan reaktörler

Şekil 4.2'de gösterilen fotoğraf, İran İslam Cumhuriyeti Cumhurbaşkanlığı Ofisi (president.ir) web sitesinde yayınlanmış ve yanlışlıkla bir düşmanın İran'ın nükleer zenginleştirme programını etkilemesi için kritik sırlardan bazılarını paylaşmıştır. Şekil 4.3, zenginleştirme işlemi için yeşil göstergelerin altındaki gri ayırıcılarla eşleşen sarı çizgilerle işaretlenmiş sahne ayrımını detaylandırır ve Mueller ve Yadegari'ye göre, Stuxnet kötü amaçlı yazılımında bulunan kodla eşleşir (Mueller ve Yadegari, 2012, s. 2). Falliere, O Murchu ve Chien, Stuxnet'in keşif ve silahlandırma sürecinin tamamlanması için "kalite güvencesi ve yönetimi gibi diğer birçok kişiyi saymayan altı ay ve beş ila on çekirdek geliştiriciye sahip olduğunu" tahmin ediyor (Falliere, O Murchu ve Chien, 2011, s. 3). Ralph Langner, "Bir Santrifüjü Öldürmek: Stuxnet'in Yaratıcılarının Başarmaya Çalıştığı Şeyin Teknik Bir Analizi" başlıklı raporunda, saldırganların, santrifüjler arasında dolaşan gerçek UF_6 da dahil olmak üzere IR-1 kaskadınının bir kopyasını inşa etmeleri gerektiğini savunuyor.

boş santrifüjlerde farklı etkilere sahip basınçlandırma ve rotor hızı manipülasyonu. Langner, yakıt zenginleştirme işleminde kullanılabilecek bileşenlerin devlet düzeyinde sıkı bir şekilde kontrol edilen ihracat malzemeleri olduğu göz önüne alındığında, Stuxnet'in yaratıcılarının devlet düzeyinde kaynaklara sahip olduklarına şüphe olmadığını savunuyor (Langner, 2013, s. 20).

Ayrıca bu aşamada, saldırganlar Realtek Semiconductor Corporation ve JMicron Technology Corporation'a ait iki meşru dijital sertifika edinmiş ve kötü amaçlı yazılımın rootkit kısmının gizlenmesi için gereken sürücüleri imzalamıştır. Stuxnet kötü amaçlı yazılımının yürütülebilir dosyalarının bulunması. Haziran 2009'daki en eski Stuxnet örneği ile Eylül 2010'daki son analiz arasında, her iki sertifika da Stuxnet'in sürücülerini imzalamak için kullanıldı. (Falliere, O Murchu ve Chien, 2011, s. 3-4). Realtek ve JMicron 'a ait her iki sertifika da iptal edildi ve uzlaşmanın keşfedilmesinin ardından yeni sertifikalar verildi. Stuxnet'in önceki bir sürümünün bu sertifikaları tehlikeye atmak için kullanılmış olması mümkün olsa da, her iki şirket de Tayvan'daki Hsinchu Bilim ve Endüstri Parkı'nda ofisler tuttu ve bu yakınlık, genellikle hava boşluğunda korunan sertifikaları çalmak için bu ofislerin fiziksel penetrasyonunu gösteriyor. ağlar (Raiu, 2010). Aleksandr Matrosov, Eugene Rodionov, David Harley ve Juraj Malcho, bir anti-virüs çözümleri şirketi olan ESET LLC tarafından yayınlanan "Stuxnet Under a Microscope: Revision 1.31" başlıklı raporlarında, bu sertifikaların bilinen botnet'lerden, yani Zeus'un sertifika çalma geçmişine sahip olduğu için diğer kaynaklardan satın alınma olasılığını vurgulamaktadır. (Matrosov A., Rodionov, Harley, and Malcho, 2011, s. 13).

Keşif ve silahlandırma sürecinden sonra, yükün hedef ağlara teslim edilmesi gerekiyordu. Şekil 4.1, ilk enfeksiyonun İran çevresinde yoğunlaştığını ve Falliere, O Murchu ve Chien tarafından yapılan kötü amaçlı yazılımın ayrıntılı analizini takiben, saldırganların başlangıçta İran'daki beş kuruluşu hedef

aldığını biliyoruz. 29 Eylül 2010 itibariyle, İran ağlarına ait konakçıların yaklaşık% 60'ı ile 100.000 bildirilen Stuxnet enfeksiyonu olmuştur. Bu şekilde tasarlanan Stuxnet, Siemens SIMATIC Step 7 yazılımı yüklü olan konakçıları tespit etmeye ve enfekte etmeye çalışır, böylece enfeksiyon İran'la sınırlı kalamaz. İlk bulaşma oluştuktan sonra, Stuxnet bir yapılandırma oluştururarak virüs bulaşmış bilgisayarın içinde blok yaparak, komut ve kontrol sunucularına teslim etmek için içeriğini şifreler. Bu veri bloğu, bilgisayarın iç ve dış İnternet Protokolü (IP) adreslerini, bilgisayarın adını, kurulu işletim sisteminin sürüm bilgilerini ve Siemens SIMATIC Adım 7 ICS yazılımını çalıştırıp çalıştırmadığını içerir (Falliere, O Murchu, and Chien, 2011, pp. 3-7). Daha önce de belirtildiği gibi, Falliere, O Murchu ve Chien'in raporuna göre, İran'ın varlığına sahip beş örgüte karşı ilk saldırılar, 22 Haziran 2009 ile 14 Nisan 2010 tarihleri arasında süren üç özel dalgada gerçekleşti. Symantec Corporation tarafından kurtarılan 3.280 örnekten en çok bildirilen Stuxnet varyantı, 01 Mart 2010'da başlatılan ikinci dalgaya aitti ve bu da muhtemelen ilk yük teslimatı sırasında sağlanan yanlış güvenlik hissi veren çalıntı sertifikalardı. (Falliere, O Murchu ve Chien, 2011, ss. 7-10).

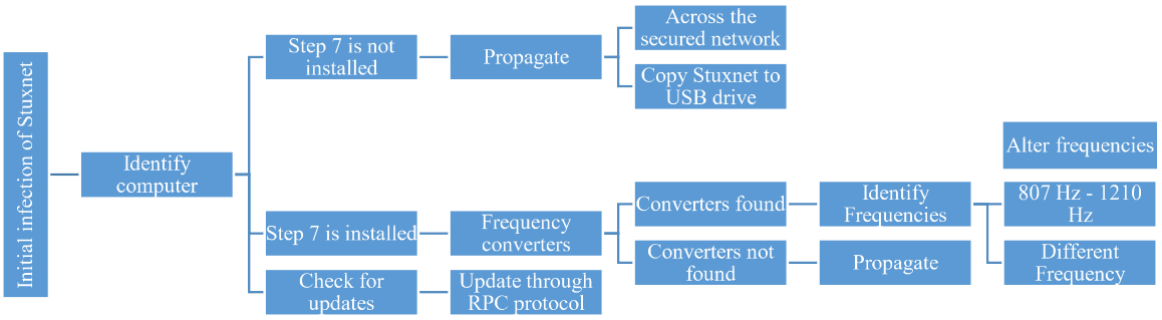
.Stuxnet'in Natanz Zenginleştirme Tesisi'nde kurulu PLC'lerin kontrolünü nasıl ele geçirebildiğini incelemeden önce, bir kontrol bilgisayarı ile bir PLC ünitesi arasındaki bağlantıyı açıklamak yararlı olacaktır. Stuxnet'in durumunda Siemens'in Adım 7 kontrol yazılımı ile yüklenen bir kontrol bilgisayarı, bir veri kablosu aracılığıyla bir PLC ile bağlantı kurar ve iki bilgisayar arasındaki iletişim Adım 7 aracılığıyla gerçekleştirilir. Stuxnet'in santrifüjleri yok edebildiği halde, kaynak koduna tam erişime sahip olmayı gerektireceği için PLC'lerin kendilerine hiçbir zaman bulaşmadığını belirtmek gerekir.

PLC'lerin çalıştırılmasının yerine, Stuxnet, kontrol bilgisayarı ile PLC arasında iletilen verileri engellemek için genellikle eski Microsoft Windows sürümlerini kullanan kontrol sistemlerini hedef aldı. Kontrol bilgisayarı, PLC'leri programlamak için Deyim Listesi (STL) veya Yapılandırılmış Kontrol Dili (SCL) gibi farklı diller kullanır. Programlandıktan sonra, PLC'ler kontrol bilgisayarı olmadan bağımsız modda çalışabilir. Bununla birlikte, uranyum zenginleştirme durumunda, santrifüj kaskadının sürekli izlenmesi ve denetlenmesi gereklidir. Eric Chien'in 2010 yılındaki raporunda keşfedildiği ve yayınlandığı gibi, Stuxnet, biri Finlandiya'da bulunan, diğeri İran'da bulunan iki özel satıcı tarafından üretilen frekans dönüştürücü sürücülerle Adım 7'yi çalıştıran bilgisayarların okuma ve yazma işlevlerini devralmak için kullanıldı.

Stuxnet bu frekansları değiştirmeye başlamadan önce 807 Hz ila 1210 Hz arasında. Bu frekanslar uranyum izotopları olanU^{235} ve $U^{238'i}$ ayırmak için tasarlanmış bir gaz santrifüjü için spesifik çalışma frekanslarıdır. Chien'in raporuna göre Stuxnet, bu santrifüjlerin frekanslarını 2 Hz'e ve daha sonra 1064 Hz'e değiştirerek sabotaj hedefine aylar içinde ulaştı (Chien, 2010). Bu da, David Albright, Paul Brannan ve Christina Walrond'un Bilim ve Uluslararası Güvenlik Enstitüsü (Albright, Brannan, ve Walrond, 2011, s. 3).

4.1.1.2 Stuxnet'in Sonrası

Daha önceki bölüm, Stuxnet solucanının iç işleyişini ve güvenli bir ağ içinde nasıl yayılabildiğini ayrıntılı olarak incelemiştir. Kötü amaçlı yazılım etkinleştirmenin son aşamasında, Stuxnet hedefleri konusunda son derece seçiciydi. Analiz, Stuxnet'in hedefi dışındaki bilgisayarlara virüs bulaştırdığını, bunu hava boşluklu ve internete bağlı olmayan nihai hedefine ulaşmak için yaptığını ortaya koydu; Tüm bunlar, sonunda yükünü dağıtmak için. Bu enfeksiyonun etkileri ihmal edilebilir düzeydeydi ve solucanın neden olduğu daha önce bahsedilen Mavi Ekran Ölüm hatasına kadar, virüslü bilgisayar sistemleri için herhangi bir arıza veya enfeksiyon belirtisi yoktu.



Şekil 4.4 Bulaşma sonrası stuxnet solucanının izlediği adımlar

Şekil Stuxnet solucanının yalnızca Adım 7 kurulu makineleri değiştirmesini sağlamak için attığı adımları göstermektedir, biri Finlandiya'da diğeri İran İslam Cumhuriyeti'nde bulunan, 807 Hz ila 1210 Hz arasındaki frekans aralıklarında çalışan iki satıcı tarafından üretilen frekans dönüştürücü sürücülerini kontrol etmekte ve izleme işlemini başlattıktan sonra, Aylar boyunca, solucan santrifüjlerin frekanslarını 2 Hz veya 1410 Hz'e değiştirir ve sonunda onları yok eder.

Şu anda genel olarak bir devlet aktörü tarafından yaratılan ve konuşlandırılan ilk siber silah olarak kabul edilen şeyin ardından, yaklaşmakta olan siber savaş korkusu yaygınlaştı. Jon R.Lindsay, "Stuxnet ve Siber Savaşın Sınırları" başlıklı çalışmasında, Stuxnet'in medya kuruluşundan şu sözlerle bahseder:

"Nefes nefese kalan medya hesapları, kimseyi fiziksel olarak yaralamayan Stuxnet'i ' atom bombasının atılmasının siber eşdeğeri' ve 'yeni bir savaş çağı ' olarak tasvir etti. Kısa süre sonra, şu anda internette açıkça bulunan Stuxnet kodunun dizginsiz bir şekilde yayılması ve Natanz ve ötesine potansiyel tali hasar konusunda endişeler ortaya çıktı. Rusya'nın NATO büyükelçisinin endişelendiği gibi, 'Bu 'mayınlar' yeni bir Çernobil'e yol açabilir." (Lindsay, 2013, s. 366).

4.1.2 Duqu

Daha önce de belirtildiği gibi, Stuxnet uranyum zenginleştirme amacıyla kullanılan yaklaşık 1.000 gaz santrifüjünü imha etmeyi başarmıştı. Buna karşılık, Duqu casusluk odaklı bir kötü amaçlı yazılımdır. Bu projenin önceki bölümlerinde tanımlanan bir siber silahın önceki tanımlarını hatırlayarak, Duqu veri bütünlüğünü etkilemez ve bu nedenle açıkça bir siber silah olarak sınıflandırılamaz.

Macar Kriptografi ve Sistem Güvenliği Laboratuvarı (CrySyS), 2011 yılında Duqu ile ilgili ilk report ve takip raporlarını yayınladı, aynı yıl Stuxnet'in etkileri bilgisayar bilimleri alanındaki güvenlik araştırmacıları tarafından anlaşıldı. Dünyanın dört bir yanındaki güvenlik araştırmacıları, Duqu ve Stuxnet'in aynı kötü amaçlı yazılım ailesine ait olduğu veya Duqu'nun geliştiricilerinin Stuxnet'in kaynak koduna erişebildiği konusunda iki olasılık üzerinde anlaştılar.

Duqu, " ~ DQ" ile dosya oluşturan kötü amaçlı yazılımlar nedeniyle adını aldı. Suçlanan taraflardan hiçbiri siber silahın yapımında sorumluluk üstlenmese de, Stuxnet'in gerçekten de devlet düzeyinde kaynaklara ihtiyaç duyduğunu tespiti yapılmıştır.

4.1.2.1 Santrifüj Sabotajına Karşı Veri Sızıntısı

Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, Márk Félegyházi, " Stuxnet'in Kuzenleri: Duqu, Flame ve Gauss" başlıklı çalışmalarında, Eylül 2011'de Avrupalı şirket, güvenli ağlarında uygunsuz birini tespit etmek için CrySyS'den yardım istedi. Bu araştırma sırasında, Bencsáth ve ark., Stuxnet'in aksine, Duqu'nun programlanabilir mantık denetleyicileri (PLC) ile ilgili herhangi bir kod içermediğini, bunun yerine Microsoft Windows tabanlı bilgisayarları hedef alan bir bilgi çalma araç setine sahip olduğunu keşfetti.

Duqu'yu parçalara ayıran güvenlik görevlileri tarafından kurulduğu gibi, Duqu bulaştığı herhangi bir sisteme zarar vermeye çalışmaz. Bunun yerine, Duqu'nun ana hedefi, virüslü sistemin Uzaktan Erişim Araçları tarafından uzaktan kontrol edilebilmesini ve hedeflenen kuruluşların özel olarak seçilmesini ve ilk müdahalenin yapılmasını sağlamaktır. kötü amaçlı bir Microsoft Word belgesiyle mızrak kimlik avı yöntemi kullanıyordu.

Şekil 4.5 Duqu rapor edilen ülkelerin Coğrafi dağılımı

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	C-Media
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	✗ (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	?	✓
Special “magic” keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Usage of LZO lib	?	✓ multiple
Visual C++ payload	✓	✓
UPX compressed payload,	✓	✓
Careful error handling	✓	✓
Deactivation timer	✓	✓
Initial Delay	? Some	✓ 15 mins
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

Şekil 4.6 Stuxnet ve Duqu Özelliklerinin Karşılaştırılması

Duqu ve Stuxnet, hem kötü amaçlı yazılımın kod yönlerinde hem de ilk izinsiz giriş aşamasının yürütülmesinde bazı önemli benzerlikler paylaşıyor. Yani, her iki kötü amaçlı yazılım da algılanmaktan kaçınmak için meşru yazılım bileşenlerinin kimliğine bürünmek için geçerli sertifikalar kullanır.

Duqu'nun yaratıcıları, kötü amaçlı yazılımlarının komuta ve kontrol yönlerini geliştirmiş gibi görünüyordu. Duqu'nun bağlantı hedefleri, önceden yapılandırılmış iki web sunucusuna bağlanmak yerine, komut ve kontrol altyapısını geliştirmek amacıyla bağlantıyı gerçek komut ve denetim sunucularına veya diğer proxy sunucularına aktaran proxy sunucularıdır. Stuxnet'in komuta ve kontrol sürecinde daha önce bahsedilen Stuxnet, kötü amaçlı yazılımın configuration dosyasına gömülü iki sabit kodlu sunucuya sahipti. Bu keşfin ardından İran, kötü amaçlı yazılımı komuta ve kontrol

sunucularından ayırarak Stuxnet'in daha da yayılmasını hızlı bir şekilde kontrol altına alabildi (Falliere, O Murchu, and Chien, 2011, p. 7). Duqu'nun varlığının kamuya açık bir şekilde keşfedilmesinin ardından, sanal makinelerde çalışan tüm proxy sunucuları, 20 Ekim 2011'de kaldırıldı ve zaten kısıtlanmış olan soruşturma seçeneklerini daha da sınırladı.

Stuxnet ve Duqu'nun yerleşik farklılıkları, Duqu'nun bulaştığı bilgisayardan aşağıdaki bilgileri çalmak için kullanılmasıyla daha da netleşir :

Duqu şunları toplar:

> "(1) Çalışan işlemlerin, hesap ayrıntılarının ve etki alanı bilgilerinin listeleri; (2) Drive adları ve ortak drive'larınkiler de dahil olmak üzere diğer bilgileri; (3) Ekran görüntüleri; (4) Ağ bilgileri (arayüzler, yönlendirme tabloları, paylaşımlar listesi, (5) Tuş basıları; (6) Açık pencere adları; (7) Numaralandırılmış paylar; (8) Çıkarılabilir sürücüler de dahil olmak üzere tüm sürücülerde dosya araştırması; (9) Etki alanındaki bilgisayarların NetServerEnum aracılığıyla numaralandırılması " (Symantec Security Reponse, 2011, s. 17).

Stuxnet ve Duqu arasındaki son fark, yukarıda belirtilen modül indirmeleri yoluyla kötü amaçlı yazılımın ömrünü uzatma yeteneği ile birlikte gelir. Duqu, gelişmiş kalıcı kampanya kullanım ömrünün sonu olarak kabul edilirse, kendisini virüslü ana bilgisayarlardan çıkarmak için kendi kendine kaldırma protokolü ile donatılmıştır (Symantec Security Reponse, 2011, pp. 18-19).

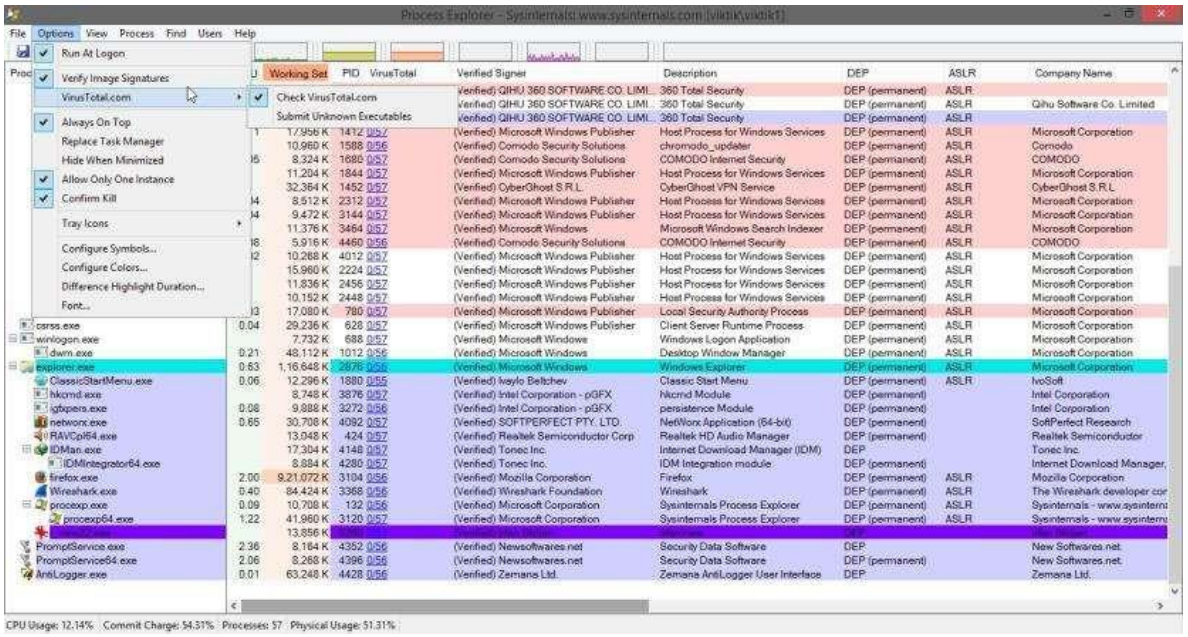
4.1.2.2 Çalınan Verilerin Etkileri

Önceki bölümde, Duqu'nun mızrak kimlik avı yöntemiyle enfekte olan bir ev sahibi saldırgandan elde etmek üzere programlandığı bazı bilgiler ayrıntılı olarak açıklanmıştır. Bu bölümde, saldırganların sızdırdığı bu bilgilerin neler başarmalarını sağlayabileceği incelenecektir.

4.1.2.2.1 İşlem Listesi, Hesap Ayrıntıları, Etki Alanı Ve Ağ Bilgileri

Doldurulmuş işlem listeleri, bir bilgisayar sisteminde kullanılmakta olan işlemler hakkında ayrıntılı bilgiler içerir. Tek başına bu bilgi, iç etki alanındaki bir bilgisayarın amacını ortaya çıkarabilir, çünkü görev odaklı bilgisayarlar bu özel görevle ilgili yazılım çalıştırıyor olacaktır. Bu görev, programlanabilir mantık denetleyicilerini (PLC) kontrol etmekten, korunan bir kompleks içindeki güvenlik kameralarını çalıştırmaya kadar değişebilir. Aşağıdaki şekil, bir Microsoft Windows işletim sisteminin tipik olarak çalıştırdığı işlemler hakkında hazır bulunan bazı bilgileri göstermektedir. Bu bilgiler aynı zamanda şu anda dağıtılan son kullanıcı sistem koruma yazılımlarını, yani anti-virüs programlarını veya ana bilgisayar tabanlı yazılımları da içerir. Bu bilgiler, bir saldırganın sistemden daha etkili bir

şekilde yararlanabilmesi için gerekli arka plan bilgilerini sağlar.



Şekil 4.7 Process Explorer Yazılımı

Hesap ayrıntıları, kaydedilen kullanıcı adları ve parolalar hakkında değerli bilgiler içerir. Şu anda sızmış olan bilgisayarın ağ sürücülerine erişim izni varsa, saldırgan yanal hareket yeteneklerini geliştirmek için bu bilgiyi edinir. Bu, sağlanan etki alanı bilgileriyle birleştirildiğinde, güvenliği ihlal edilen kimlik bilgilerinin temizleme düzeyine bağlı olarak ağın tamamen tehlikeye girmesine neden olabilir. Ağ bilgileri, aynı ağ içindeki tüm erişilebilir bilgisayarların, yönlendiricilerin, güvenlik duvarlarının ve ağa erişilebilir tüm siber alan uygulamalarının IP adresleri hakkında veriler içerir. Bu aletlerin üreticileri, seri numaralarını, hangi işletim sistemlerini kullandıklarını ve çoğu bilgisayarın belirledikleri işlevlerden sonra adlandırıldığı göz önüne alındığında, hizmet ettikleri işlev ağ içinde de saldırganlara bildirilir.

4.1.2.2.2 Yerel Sürücüler Ve Ağ Sürücüleri

Saldırgan güvenliği ihlal etmişse yeterince yüksek açıklık, ağ ortak sürücülerinin içeriğine de bu bilgi parçası aracılığıyla erişilebilir. Bunu takiben, saldırgan belirli dosyaları sızdırmayı veya dosyaları ve söz konusu dosyanın tüm kopyalarını değiştirmeyi veya yok etmeyi seçebilir.

4.1.2.2.3 Ekran Görüntüleri Ve Tuşlara Basma

Şekil 4.7 aynı zamandaMicrosoft'un Windows işletim sistemi olan bir bilgisayar sisteminin ekran görüntüsüdür. Ekran görüntüsü, bilgisayar ekranında görüntülenenlerin bir görüntüsüdür. Araç, son derece gizli belgeleri, bir silahın planlarını sızdırmak ve hatta bir siber silah tarafından kullanılabilecek önemli kod parçalarını çalmak için kullanılabilir. Günümüzde, şifreler doğrudan net bir şekilde görüntülenmemektedir, bu noktada, tuş kaydetme yazılımı tarafından yakalanan tuş basmaları, kullanıcının klavyesindeki her tuş vuruşu kaydını saldırgana sağlayacaktır. Kişisel bilgilerden kullanıcıame'lerine ve şifrelerden banka hesaplarına ve kredi kartı numaralarına kadar bu araçlarla sızdırılabilir.

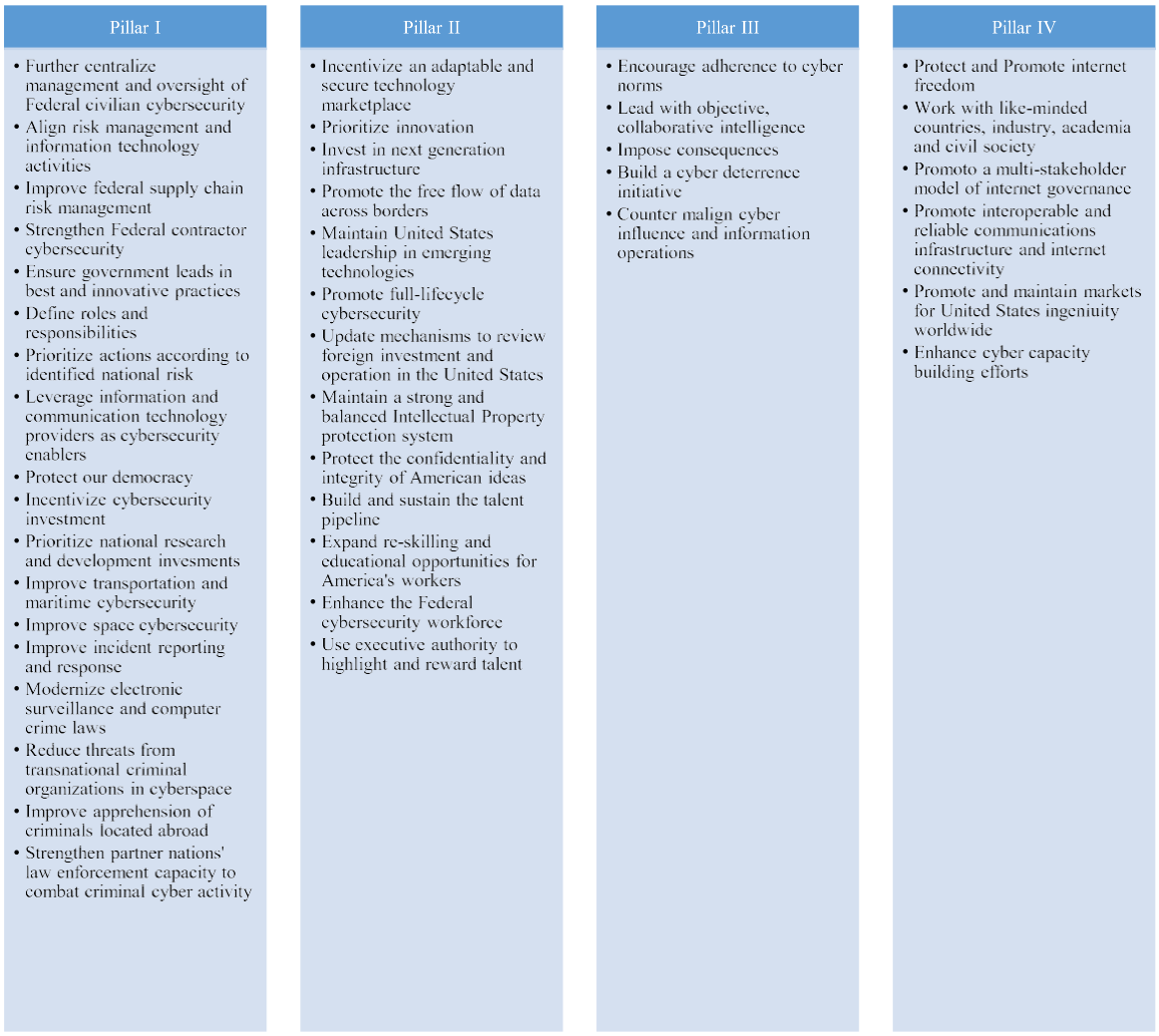
5. Batı Ülkelerinde Mevcut Siber Stratejiler

Önceki bölümler, siber uzayın sakinlerini, devleti ve devlet dışı aktörleri ilgilendiren siber tehditleri incelemiş ve tartışmıştır. Bu bölüm, devletlerin siber uzaydaki çıkarlarını güvence altına almaya yönelik devlet stratejilerine odaklanmaktadır. Bu bölüm, Batı bloğunun sadece caydırıcılık teorisine dayanması nedeniyle ortaya koyduğu stratejilere odaklanmaktadır. Stuxnet ve daha sonraki varyantı Duqu'nun Batı bloğundan ve müttefiklerinden ortaya çıktığından şüphelenildiği göz önüne alındığında, bu ülkelerin siber stratejilerini incelemek faydalı olacaktır

5.1 Amerika Birleşik Devletleri

Beyaz Saray, Eylül 2018'de Amerika Birleşik Devletleri'nin siber stratejisini detaylandıran "Amerika Birleşik Devletleri'nin Ulusal Siber Stratejisi" başlıklı bir rapor yayınladı. Amerika Birleşik Devletleri'nin görevdeki Başkanı Donald J. tarafından imzalanan rapor. Trump, "bu Ulusal Siber Stratejinin yayınlanmasıyla, ABD'nin 15 yıl içinde ilk kez tamamen ifade edilmiş siber stratejisine sahip olduğunu" iddia ediyor (Trump, 2018, s. I). Rapor, Rusya Federasyonu, İran İslam Cumhuriyeti, Kuzey Kore Halk Cumhuriyeti ve Çin Halk Cumhuriyeti'ni Amerikan uluslararası işletmelerine ve müttefiklerine karşı siber saldırılarda bulundukları için seçiyor. Raporda ayrıca, devlet dışı aktörlerin, "ifade özgürlüğü ve bireysel özgürlük" Amerikan vizyonuyla yaratılan siber alanı, "Amerika Birleşik Devletleri'ne ve müttefiklerine karşı düşman devletlerin korumasından yararlanırken kâr etmek, işe almak, propaganda yapmak ve saldırmak" için istismar ettikleri belirtilmektedir (Trump, 2018, ss. 1-2). Projenin bu bölümü, Beyaz Saray tarafından yayınlanan raporun ilgili bölümlerini, projenin önceden belirlenmiş hedefleriyle bağlantılı olarak, bu projede incelenen göreceli algılanan tehditler ve bu tehditlere karşı önlemler ile birlikte incelemektedir. Rapor, rakiplerinin ortaya koyduğu yukarıda belirtilen zorluklarla mücadele etmek için, Amerika Birleşik Devletleri'nin ulusal siber stratejisinin üzerine kurulacağı dört sütunu detaylandırıyor ve açıklıyor. "Sütun I: Amerikan People'yi, Anavatanı ve Amerikan Yaşam Tarzını Koruyun;

Sütun II: Amerikan Refahını Teşvik Etmek; Sütun III: Barışı Güç ile Korumak; Sütun IV: İleri Amerikan Etkisi" (Trump, 2018, s. V-VI).



Şekil 5.1 A.B.D. Ulusal Siber Stratejisini Dayandığı Temeller

Raporda, Trump yönetimi ilk ayağın amacını "Ulusun bilgi ve bilgi sistemlerinin güvenliğini ve esnekliğini artırmak için siber güvenlik risklerini yönetmek" olarak tanımlamaktadır (Trump, 2018, s. 6). Trump yönetimi, federal güvenliği sağlamak için ana hatlarıyla belirtilen öncelikli eylemlere odaklanarak bu hedefe ulaşmayı hedefliyor .

5.2 Avrupa Birliği

AB Siber Güvenlik Yasası, Avrupa Birliği'nin siber altyapısının hazırlığını artırmak amacıyla tehdit istihbaratı paylaşımını geliştirmek için "Pan-Avrupa Siber Güvenlik

Tatbikatları" başlıklı yıllık siber tatbikatlar önermektedir.

Planın ilk adımında AB, AB'yi siber uzayda siber suçlular tarafından kullanılan siber wea ponlara karşı savunmak için araçlar ve teknolojiler sağlamak üzere üye devlet koordinasyonunu ulusal düzeyde geliştirecek bir Avrupa Siber Güvenlik Araştırma ve Yetkinlik Merkezi kurmayı hedefliyor. Planın ikinci adımında, AB iyileştirme için bir plan operasyonel planı hazırlamayı planlıyor.

AB Siber Güvenlik Yasası, 11 Aralık 2018'de yürürlüğe girerek ENISA'nın görev süresini kalıcı olarak genişletti ve üye devletlere yönelik yardımı iyileştirmek amacıyla yeni bir siber güvenlik sertifikasyon çerçevesinin temelini oluşturdu. Amerika Birleşik Devletleri Ulusal Siber Stratejisi'ndeki en önemli konu olduğu gibi, siber güvenlikteki bilgi açığı, eğitim kaynaklarının eksikliği veya beceri açığı, en çok siber bağımlı ülkelerin bazılarının gündeminde görünmeye başlamıştır. Siber savunma ve saldırı stratejileri, siber alandaki uluslararası iş birliğini geliştirmeye ve ilk bölümlerde ele alınan siber alanın farklılıkları nedeniyle geleneksel alanların sınırlarının ötesine genişletmeye çok iyi hizmet edebilir.

6. Siber Alanın Geleceği

Günümüzde, uzaktan kumandalı insansız hava araçları (İHA), esneklikleri nedeniyle ordular arasında çok sayıda amaç için popülerlik kazanmaktadır. Bu projenin amacının tanımlandığı bölüme dönersek, alanlar arası bir manevra şu şekilde örneklendirilmiştir: "Uluslararası sularda konumlandırılmış bir taşıyıcıdan hareket eden, bilgisayar güdümlü bir füze konuşlandıran, yörüngedeki uydular aracılığıyla uzak bir bilgisayara çok sayıda veri ileten bir drone". Bu örnek, operasyonel etki alanının tüm dallarını içerir: kara, deniz, hava, uzay ve siber. Manevranın başarısı, operasyonel alanların tüm operatörlerinin birbirine bağlı olarak çalışmasına bağlıdır.

Ordular, üyelerini invaziv ve invaziv olmayan implantlar, beyin bilgisayar arayüzleri (BCI), başa monte ekranlar (HMD) yoluyla iyileştirmeye çalışabilirler. Bu yükseltmeler bile birbirine bağlı olabilir ve hatta bilgilerini İnternet'ten indirip güncelleyebilirler. Başa monte ekranlar sıradan gözlüklerin boyutuna indirgenebilir, dışarıdan gelen girdilere güvenmek yerine, bir kişinin kafatasına implante edilen veya takılan beyin bilgisayar arayüzleri aracılığıyla sistemin kontrolünü sağlayabilir. Bununla birlikte, mevcut görünüm, en azından, siber saldırı ve savunma odaklı işlerin siber devrim süresince sürekli talep görmeye devam edeceği görülmektedir.

7. Sonuçlar ve Öneriler

Bu çalışmanın siber stratejiler bölümünde incelendiği gibi, ancak şimdi beceri açığı devletler tarafından ele alınmaktadır. Kuşkusuz, bu beceri açığının giderilmesine yönelik olarak söz konusu politikaların alacağı karşı önlemlere uygun olarak gelecek nesillerin yetiştirilmesi gerekecektir.

Gelecek, gerçek bir yapay zekâ geliştirip geliştirmeyeceğimiz konusunda belirsizliğini koruyor. Olası Skynet (Terminatör filminden) senaryosunun korkuları arasında kesin olan bir şey var, bir süper-zekanın gerçeğe dönüşmesi durumunda, gelecek artık sadece insanlara ait olmayacak.

Bununla birlikte, oraya varmadan önce, multidisipliner siber uzay alanının plakasında birçok engel ve ikilem var. Siber uzayla ilgili uluslararası hukuk neredeyse hiç yoktur, alan yetişmeye çalışırken siberin alanını tamamen anarşi içinde bırakır. Bununla birlikte, siber uzay statik bir varlık değildir, zamanla değişecektir. Bazı uzmanlar, "dijital bir Pearl Harbor" un kapılarda olabileceğini, siber bağımlı yaşamın tüm alanlarının ilk önce kaosa düştüğünü iddia ediyorlar. Elbette, endüstriyel bir kontrol sabotajı başka bir Çernobil'e yol açabilir,

Önceki bölümleri özetlemek gerekirse, güvenlik hiç bitmeyen bir süreçtir. Siber güvenlik, tehditler sürekli geliştiği için daha da fazladır. Bu güvenlik yükü doğrudan sistem yöneticilerine ve siber güvenlik uzmanlarına düşmektedir, ancak bu yükü politika yapıcılar tarafından belirlenen uygun siber güvenlik stratejileri olmadan tek başlarına taşıyamazlar.

Politika yapıcıların, devlet dışı aktörlerin ve insanların ortak bir yeteneği vardır: uyum sağlama yeteneği. Hayatta kalmak ve geleceği daha iyi hale getirmek için, beşinci operasyonel alanın sunduğu zorluklara uyum sağlamalıyız.

Kaynaklar

İbrahim, S. (2018, Ocak 09). *12'den fazla kötü amaçlı yazılım türü örneklerle açıklanmıştır (tam liste)*, MalwareFox: https:// www.malwarefox.com/malware-types/

Albright, D., Brannan, P. ve Walrond, C. (2010). *Stuxnet, Natanz Zenginleştirme Tesisi'nde 1.000 santrifüj çıkardı mı?* Washington, D.C.: Bilim ve Uluslararası Güvenlik Enstitüsü.

Albright, D., Brannan, P. ve Walrond, C. (2011). *Stuxnet Malware ve Natanz: ISIS 22 Aralık 2010 Raporu Güncellemesi.* Washington, D.C.: Bilim ve Uluslararası Güvenlik Enstitüsü.

Bahmani, M. (2018, 07 Kasım). *AI vs Machine Learning vs Derin Öğrenme* Medium: https://medium.com/datadriveninvestor/ai-vs- machine-learning-vs-deep-learning-ba3b3c58c32

Baskin, B., Bradley, T., Faircloth, J., Schiller, C. A., Caruso, K., Piccard, P., . .. Piltzecker, T. (2006). Bölüm 1 - Casus Yazılımlara Genel Bir Bakış. B. Baskin, T. Bradley, *Combating* Spyware in the *Enterprise (Kuruluşta Casus Yazılımla Mücadele*) (s. 1-25). Syngress.

Bencsáth, B., Pék, G., Buttyán, L. ve Félegyházi, M. (2011). *Duqu*: *Vahşi doğada bulunan Stuxnet benzeri bir kötü amaçlı yazılım*. Budapeşte: Kriptografi ve Sistem Güvenliği Laboratuvarı (CrySyS).

Bencsáth, B., Pék, G., Buttyán, L. ve Félegyházi, M. (2012). Stuxnet'in Kuzenleri: Duqu, Flame ve Gauss. *Gelecekteki İnternet*, 971-1003. doi:10.3390/fi4040971

Bostrom, N. (2016). *Süper Zeka Yolları, Tehlikeleri, Stratejileri.* Oxford: Oxford Üniversitesi Yayınları.

Cameron, J. (Yönetmen). (1984). *Terminatör* [Sinema Filmi].

Chen, P., Desmet, L. ve Huygens, C. (2014). Gelişmiş Kalıcı Tehditler Üzerine Bir Çalışma

Chien, E. (2010, 12 Kasım). *Stuxnet: Bir Atılım*. Symantec

Christou, G. (2016). *Avrupa Birliği'nde Siber Güvenlik Yönetişim Politikasında Dayanıklılık ve Uyarlanabilirlik* . Hampshire: Palgrave Macmillan.

Clarke, R. A. ve Knake, R. (2010). *Siber Savaş: Ulusal Güvenliğe* Bir Sonraki Tehdit *ve* Bu *Konuda Ne Yapmalı?* New York, NY: HarperCollins.

Dando, M. (2015). Sinirbilim İlerlemeleri ve Gelecekteki Savaş. J. dilinde Clausen ve N. Levy, *Nöroetik El Kitabı* (s. 1785-1800). New York: Springer Science + Business Media Dordrecht.

Davis, S. E. ve Smith, G. A. (2019). Savaşta Transkraniyal Doğru Akım Stimülasyon Kullanımı: Faydalar, Riskler ve Gelecekteki Beklentiler. *İnsan Sinirbiliminde Sınırlar*, *13*, 1-18. doi:10.3389/fnhum.2019.00114

Eggenschwiler, J. ve Silomon, J. (2018). Siber silah norm yapımındaki zorluklar ve fırsatlar. *Bilgisayar Dolandırıcılığı ve Güvenliği, 2018*(12), 11-18. doi:10.1016/S1361-3723(18)30120-9

Falliere, N., O Murchu, L. ve Chien, E. (2011, Şubat 11). *W32. Stuxnet Dosyası.* Erişim tarihi: 15 Haziran 2019, Symantec: https:// www.symantec.com/content/en/us/enterprise/media/security_response/white papers/w32_stuxnet_dossier.pdf

Fontugne, R., Bautista, E., Petrie, C., Nomura, Y., Abry, P., Goncalves, P.,. . . . Aben, E. (2019). BGP Zombies: A Nalysis of Beacons Stuck Routes. D. Choffnes ve M. Barcellos (Ed.), *Pasif ve Aktif Ölçüm. PAM 2019. Bilgisayar Bilimlerinde Ders Notları. 11419*, s. 197-209. Cham: Springer.

Ford, R. (1999). Kötü Amaçlı Yazılım: Troya Yeniden Ziyaret Edildi. *Bilgisayar ve Güvenlik,* 18(2), 105-108. doi:10.1016/S0167-4048(99)80027-3

Gediya, J., Singh, J., Kushwaha, P., Srivastava, R. ve Wang, Z. (2019). 7 - Açık Kaynak Kodlu Yazılım. R. Oshana ve M. Kraeling (Eds.), *Gömülü Sistemler için Yazılım Mühendisliği* (s. 207-244). Cambridge, MA: Elsevier.

Gibney, A. (Yönetmen). (2014). *Zero Days* [Sinema Filmi]. Gibson, W. (1984). *Neuromancer*. New York: As.

Goodin, D. (2016, Eylül 29). *Rekor kıran DDoS'un >145k saldırıya uğramış kameralar tarafından* teslim *edildiği bildirildi*. Ars Technica: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras- reportedly-deliver-internets-biggest-ddos-ever/

Hallett, M. (2007). Transkraniyal Manyetik Stimülasyon: Bir Astar. *Nöron*, 187-199. doi:10.1016/j.neuron.2007.06.026

Herzog, S. (2011). Estonya Siber Saldırılarını Yeniden Ele Almak: Dijital Tehditler ve Çok Uluslu Yanıtlar. *Stratejik Güvenlik Dergisi, 4*(2), 49-60. doi:10.5038/1944-0472.4.2.3

Uluslararası Telekomünikasyon Birliği. (1994, Temmuz 01). *ITU-T Öneriler Veritabanı.*, Uluslararası Telekomünikasyon Birliği

Kaplan, J. (2016). *Yapay Zeka: Herkesin Bilmesi Gerekenler*. Yeni York: Oxford Üniversitesi Yayınları.

Keane, S. (2019, 15 Temmuz). *Huawei yasağı: Telefonlarının nasıl ve neden ateş altında olduğuna dair tam zaman çizelgesi*. Cnet: https:// www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire/

Kuehl, D. T. (2009). Siber Uzaydan Siber Güce: Sorunu Tanımlamak. F. D. içinde. Kramer, S. H. Starr ve L. K. Wentz (Eds.), *Siber Güç ve Ulusal Güvenlik* (s. 24-42). Washington, D.C.: Potomac Kitapları.

Langner, R. (2013). *Bir Santrifüjü öldürmek için.* Arlington: Langner Grubu.

Libicki, M. C. (2009). Siber *caydırıcılık ve Siber Savaş.* Santa Monica, Kaliforniya: RAND.

Lindsay, J. R. (2013). Stuxnet ve Siber Savaşın Sınırları. *Güvenlik Çalışmaları, 22*(3), 365-404. doi:10.1080/09636412.2013.816122

Liska, A. ve Gallo, T. (2017). *Dijital Gasp Karşı Savunma Fidye Yazılımı*. Sebastopol, CA: O'Reilly.

Lysne, O. (2018). *Huawei ve Snowden Soruları, Güvenilmeyen Satıcılardan Elektronik Ekipman Doğrulanabilir mi? Güvenilmeyen Bir Satıcı Elektronik Ekipmana Güven Oluşturabilir mi?* Cham: Springer.

Özgeçmiş

Adı Soyadı:	Fikret GÜNGÖR
E-mail (1):	y210234065@ogr.ikc.edu.tr
E-mail (2):	fikretgungor@gmail.com

Eğitim:

1998-2002	Hava Harp Okulu Bilgisayar Mühendisliği Bölümü
2003-2004	MEBS Subaylığı Temel Eğitimi

İş Deneyimi:

2003 - Halen	Hava Kuvvetleri Komutanlığında Bilgi Sistemleri Subayı (2’nci Ana Jet Üs Komutanlığı/Çiğli)