T.C.
HİTİT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI

SİBER SAVAŞLARIN ETKİLERİ İLE DEVLETLERİN GÜVENLİK STRATEJİLERİ

Yüksek Lisans Tezi

MUHAMMET FATİH AYKURT

Çorum - 2023

SİBER SAVAŞLARIN ETKİLERİ İLE DEVLETLERİN GÜVENLİK STRATEJİLERİ

MUHAMMET FATİH AYKURT

Lisansüstü Eğitim Enstitüsü

Adli Bilimler Anabilim Dalı

Yüksek Lisans Tezi

TEZ DANIŞMANI

Dr. Hakan KÖR

Çorum 2023

KABUL ONAY SAYFASI

Muhammet Fatih AYKURT tarafından hazırlanan "**Siber Savaşların Etkileri ile Devletlerin Güvenlik Stratejileri**" adlı tez çalışması 27/01/2023 tarihinde aşağıdaki jüri üyeleri tarafından oy birliği/oy çokluğu ile Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Adli Bilimler Anabilim Dalında Yüksek Lisans Tezi olarak kabul edilmiştir.

Doç. Dr. Akif AKGÜL ……

Dr. Öğr. Üyesi Hakan KÖR ……

Dr. Öğr. Üyesi Fahrettin HORASAN ……

Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun …/…/…… tarih ve …….. sayılı kararı ile Muhammet Fatih AYKURT'un Adli Bilimler Anabilim Dalında Yüksek Lisans derecesi alması onanmıştır.

(İmza)

Prof. Dr. Muhammed Asıf Yoldaş

Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını beyan ederim.

(İmza)

Muhammet Fatih AYKURT

SİBER SAVAŞLARIN ETKİLERİ İLE

DEVLETLERİN GÜVENLİK STRATEJİLERİ

MUHAMMET FATİH AYKURT

ORCID:0000-0002-2698-3952

HİTİT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Yüksek Lisans

OCAK 2023

ÖZET

Yaşamış olduğunuz çağda bilgisayar ve telekomünikasyon alanında yaşanan değişim teknolojiye olan bağlılığı artırmıştır. Dijital teknolojiler internetin ortaya çıkması ile hızla bir gelişim göstermiştir. İnternet hayatı kolaylaştıran faydalarının yanında birtakım sorunları da beraberinde getirmiş, yeni bir saldırı ortamı oluşturmuştur. İletişimin merkezi olan internetin kötü amaçlı olarak kullanılması da engellenemez hale gelmiştir Bu alanda dünyamızda ulusal ve uluslararası boyutta siber saldırı, siber savaş ve siber güvenlik gibi kavramlar ortaya çıkmıştır. Yapılan saldırılar sonrası ülkelerin güvenlik otoriterileri bu alandan gelen saldırılara ilişkin savunma stratejileri geliştirmeye başlamıştır.

Hazırlamış olduğum bu tez çalışmasında ülkeler ve uluslararası örgütler ile ulusal ölçekte siber savaş boyutunda yaşanan saldırılara örnekler verilmiş sonrasında ise ekonomik, siyasi, toplumsal ve medya boyutları incelenerek siber savaşın bu alanlara etkisi araştırılmıştır. Daha sonra ise ülkelerin ayrı ayrı savunma stratejilerine değinilmiştir.

Anahtar Kavramlar: Siber Saldırı, Siber Savaş, Siber Uzay, Siber Güvenlik, Kritik Alt Yapılar

Bilim Kodu: 90102, 92403

WITH THE EFFECTS OF CYBER WARS

SECURITY STRATEGIES OF STATES

MUHAMMET FATİH AYKURT

ORCID: 0000-0002-2698-3952

HITIT UNIVERSITY

GRADUATE SCHOOL

Master of Science

OCTOBER 2023

ABSTRACT

The change in the field of computers and telecommunication in the era you live in has increased the commitment to technology. Digital technologies have developed rapidly with the emergence of the internet. In addition to the benefits that make life easier, the Internet has brought some problems with it and created a new attack environment. The malicious use of the internet, which is the center of communication, has also become unavoidable. In this field, concepts such as national and international cyber attacks, cyber warfare and cyber security have emerged in our world. After the attacks, the security authorities of the countries started to develop defense strategies for attacks from this area.

In this thesis that I have prepared, examples of attacks in the dimension of cyber warfare on a national scale with countries and international organizations are given, and then the effects of cyber war on these areas are investigated by examining the economic, political, social and media dimensions. Then, the defense strategies of the countries are mentioned separately.

Key Terms: Cyber Attack, Cyber War, Cyberspace, Cyber Security, Critical Infrastructures

Science Code: 90102, 92403

TEŞEKKÜR

Yüksek lisans tez çalışmam süresince desteğini hiç esirgemeyen, tecrübesi ile şahsımın bu tezi hazırlamasında ilgi, önerilerini sunmaktan kaçınmayan, tezin hedeflenen sonuca ulaşması için büyük emekleri olan değerli danışman hocam Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Anabilim Dalı Başkanı Sayın Dr. Öğr. Üyesi Hakan KÖR hocama ve bu süreçte beni sürekli motive eden ve yanımda olan değerli eşime teşekkür ve saygılarımı sunarım.

Av. Muhammet Fatih AYKURT

İÇİNDEKİLER

3.BÖLÜM

SİBER SAVAŞ VE ETKİLERİ

TABLOLAR DİZİNİ

Tablo **Sayfa**

ŞEKİL DİZİNİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Simgeler

%	Yüzde

Kısaltmalar

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AR-GE	Araştırma Geliştirme
BM	Birleşmiş Milletler
BT	Bilgi Teknolojileri
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
Bkz.	Bakınız
CYBERCOM	Siber Komutanlık
DEAŞ	Irak Şam İslam Devleti (Dawlah al-Islamiyah fil-'Iraq wa ash-Sham)
DNS	Alan Adı Sağlayıcısı (Domain Name System)
DDos	Dağıtık Servis Dışı Bırakma Saldırısı (Distributed Denial of Service)
DoS	Servis Dışı Bırakma (Denial of Service)
DSİ	Devlet Su İşleri
FBI	Federal Araştırma Bürosu (Federal Bureau Of Investigation)
LAN	Yerel Alan Ağı
NATO	Kuzey Atlantik Anlaşması Örgütü
NSA	Amerikan Ulusal Güvenlik Ajansı
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TC	Türkiye Cumhuriyeti
TCK	5237 sayılı Türk Ceza Kanunu

IP	İnternet Protokolü (Internet Protocol)
MTA	Maden Tetkik ve Arama Enstitüsü
ODTÜ	Orta Doğu Teknik Üniversitesi
RADAR	Radyo Tespit Etme ve Menzil Tayini
RTÜK	Radyo Televizyon Üst Kurulu
SCADA	Merkezi Denetim Ve Veri Toplama (Supervisory Control And Data Acquisition)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
TCK	Türkiye Cumhuriyeti Karayolları
vb.	Ve Benzeri
vs.	Vesaire
YÖK	Yükseköğretim Kurulu
yy.	Yüzyıl

GİRİŞ

İnsanlığın var oluşundan bu yana bireylerin, toplumların ve devletlerin varlığını sürdürebilmek için ilk hedefi kendini korumak ve güvenliğini sağlamak olmuştur. Geçmişten bugüne kadar insanlar bu amaçla silahlanmış ve ordular kurmuştur. İlk çağlardan bu yana süre gelen bu içgüdüsel anlayış çerçevesince alınan tedbirler zamana, mekâna ve teknolojinin gelişmesine bağlı olarak değişim göstermiştir.

İnsanoğlu bilgi ve iletişim teknolojilerinin gelişmesine bağlı olarak kendini korumak, varlığına tehdit olarak gördüğü yapılara karşı savunma ve saldırılar yapmak üzere çeşitli silahlar geliştirmiştir. Bu kapsamda ilk dönemlerde yakın mesafe silahlarla savunma yapan saldırılar düzenleyen toplumlar teknolojiye bağlı olarak uzaktan saldırı ve savunma yapabilir hale gelmiştir. Günümüz dünyasında artık savunma ve saldırıların tek bir tuş ile yapıldığı herkesin malumu olup bireyler ve devletler buna göre savunma stratejileri geliştirmektedir.

Yaşamış olduğunuz bu çağda bilgisayar ve telekomünikasyon alanında yaşanan değişim teknolojiye olan bağlılığı artırmıştır. Fiziksel sınırların neredeyse ortadan kalktığı bu dönemde yaşanan gelişim ve kolaylıklar sorunları da beraberinde getirmiştir. İletişimin merkezi olan internetin kötü amaçlı olarak kullanılması da engellenemez hale gelmiştir. Bu kapsamda devletlerin yaşamış oldukları sıkıntıların etkilerine dikkat çekmek ve alınması gereken önlemleri değerlendirmek adına yaşanan siber olaylardan yola çıkılarak bu çalışma hazırlanmıştır.

Bu çalışma ile geleneksel savaş kavramından soyutlandığımız bir dönemde telekomünikasyon alanında gerçekleşen gelişmelerle siber savaşların ülkelerin siyasi, ekonomik ve toplumsal yapılarına etkilerini incelenmiş ayrıca medya üzerinden oluşturulan algılara değinilmiştir. Bununla birlikte ülkelerin siber savaşlara karşı nasıl bir güvenlik stratejisi geliştirmeye çalıştığı incelenerek yapmış oldukları çalışmalar analiz edilmiştir.

Bu tez çalışmasının amacı bireysel siber saldırılardan ziyade devletlerin kara, deniz, hava ve uzay alanının tamamını içine alan yeni bir savaş alanı ile karşı karşıya olduklarını ortaya koymaktır. Siber saldırılar sonucu devletlerin hangi tür tehlikelerle karşı karşıya kaldıkları örneklem analiz yöntemi ile değerlendirilip çeşitli yönlerden etkileri araştırılıp bilimsel veriler ile desteklenmiştir. Buna mukabil olarak devletlerin güvenlik stratejileri de incelenerek yeni bir savaş alanı olan siber uzaydaki güç dengeleri karşılaştırılmıştır

1.BÖLÜM
SİBER ORTAM VE KAVRAMSAL ÇERÇEVE

Günümüz dünyasında yaşanan teknolojik gelişmelerin etkisiyle 20. yy içerisinde yeni bir kavram olarak hayatımıza giren siber alandan ve bu yeni gelişen alanın olumlu olumsuz etkilerinden bahsedilmeden önce konu ile bağlantılı kavramlar ayrıntıları ile aşağıda açıklanmıştır.

1.1. Siber Kavramları

"Siber" kelimesi Antik Yunan kökenli bir kelime olup İngilizce "Cyber" kelimesinden uyarlanarak "bilgisayar ağlarına ait olan" veya "sanal gerçeklik" anlamında kullanılmaktadır. Siber kavramı ilk ortaya çıktığı dönemde karmaşık sistemlerin kontrolü gibi tanımlanmış ise de daha sonraki dönemlerde tüm telekomünikasyonu, interneti, bilgisayar sistemlerini, fiber optik kabloları içine alan geniş bir alan olarak tanımlanmıştır. Ancak farklı tanımları da zaman içerisinde yapılmaya devam edilmektedir.

Her toplum sibernetik tarihinde kendi yetiştirdiği ilim adamlarıyla gurur duymuştur. Fransızlar matematik dehası olarak gördükleri Pascal (Paskal) ve ünlü düşünür Descartesile övünürler. İngilizler ise bilgisayar biliminin babası olarak kabul edilen Charles Babbage'nin sibernetiğe öncü olduğunu ileri sürerler. Almanların ise öne sürdükleri kişi Leibniz'dir. Oysaki Ebu'l-İz El Cezeri bundan yaklaşık 9 asır önce Otomatik Kontrol Bilimi'ni kurmuştur. Bilgisayar bilimi ve Sibernetik denildiğinde ilk bilgin müslüman Ebu'l İz İsmail İbni Rezzaz El-Cezeri'dir (1136-1233). Sibernetik yani robotik alanının öncüsü olarak kabul edilen, robot ve ustası, fizikci, bilim adamı Ebu'l İz El-Cezeri 44'den fazla buluş yapmıştır. El Cezeri'nin yapmış olduğu otomatik saat, su pompalama sistemi ve otomatik abdest alma makinası tarihteki ilk robotlar olarak kayıtlara geçmiştir. Bizlerde Sibernetiğin ilk çıkış sürecini canlı ve cansız karmaşık tüm sistemleri yöneten ve denetleyen bir bilim dalı olarak kabul eder ve ülkemiz tarihi ve İslam tarihi bir bütün olarak değerlendirildiğinde El Cezeri sibernetiğin kurucusu olarak kabul edilmektedir. (Köprülü,2020, s.16).

Günümüzde ise siber terimi bilgisayar ağları ile ilişkilendirilerek kullanıldığı için günümüz anlamına yakın olarak ilk kez Norbert Wierner'in 1948 yılında yazdığı "Sibernetik: Makineler ve Hayvanlar Arasında Kontrol Ve İletişim" isimli eserinde kullanılmıştır. Kitap içerisinde siber terimi mekanik ağlar ve karışık sistemlerin kontrolünü ifade etmektedir. (Avcıoğlu, 2017,s33-34) Sibernetik biliminin bu şekilde tarif edilmesi özellikle 2. Dünya Savaşı sırasında taraflar arasındaki yoğun hava saldırılarına karşı insan kontrolünde olan hava savunma sistemlerinin hızlı ve hassas bir şekilde çalışmasına duyulan ihtiyaçtan doğmuştur. İnsanlar tarafından mekanik olarak kontrol edilmesi imkansız olan radar antenlerinin hedeflere otomatik olarak dönmesi ve hedefini kendi kendine bulup vuran uçaksavar toplarına (füzelerine) duyulan

gereksinimler sibernetik bilime olan ihtiyacı ve bu bilimin gelişmesine yönelik çalışmaları daha da hızlandırmıştır.

1.1.1. Siber Uzay

Türkiye Cumhuriyeti 2020-2023 Siber Eylem Planında "Siber Uzay" kavramı dolaylı ya da doğrudan olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler şeklinde tanımlanmıştır. Ulaştırma Bakanlığı Eylem Planı, 2020, s.10) Amerikan Savunma Başkanlığı ise "Siber Uzay" kavramını internet, telekomünikasyon ağları, bilişim sistemleri, kapalı işlemci ve kontrol mekanizmalarını da içerisine alan, birbiriyle bağlantılı bilişim teknolojisi alt bileşenlerinden oluşan küresel bir mekan olarak tanımlamaktadır. Siber uzayın yukarıda belirttiğimiz tanımlardan anlaşılacağı üzere genel bir tanımını yapılacak olursa tüm telekomünikasyon ve elektromanyetik sistemleri içine alan, kara, deniz, hava ve uzaydaki tüm sistemlerle iç içe geçmiş bulunan alan olarak tarif edilebilir.

1.2. Siber Saldırı

Özellikle internet ağının tüm dünyada yaygınlaşması, bilişim sistemlerinin hızlı gelişimi sonrası bu alanda taraflar arasındaki anlık bilgi transferleri hayatımızı çok kolaylaştırmıştır. Ancak bu alanda gelen kolaylıklar beraberinde açıklar oluşturmuş ve gerek fertler gerekse toplumları yöneten devletler tarafında karşı tarafın aleyhine olacak şekilde kullanılmaya başlanmıştır. Bu sebeple siber saldırı denildiğinde, siber uzay kavramı içerisinde değerlendirdiğimiz tüm alanlarda bir kişi veya grup tarafından bilişim sistemleri kullanılarak, karşı tarafın alanına yapılan yetkisiz erişimi, kurum veya şirketleri dezenformasyona uğratmak için yapılan girişim, yapılacak olan hizmetlerin engellenmesi, kullanılamaz hale getirilmesi, kişilerin veya kurumların verilerinin çeşitli menfaatler için çalınması, değiştirilmesi veya yok edilmesinin bir bütünü olarak tanımlayabiliriz. T.C. 2020-2023 Siber Eylem Projesinde ise siber saldırılar siber alandaki endüstriyel ve bilişim kontrol sistemlerinin veya bu sistemler aracılığıyla tutulan verinin ortadan kaldırılması amacıyla, siber uzayın herhangi bir yerindeki kişi veya sistemler tarafından kasıtlı olarak yapılan işlemler olarak tanımlanmıştır (Ulaştırma Bakanlığı Eylem Planı, 2020, s.10).

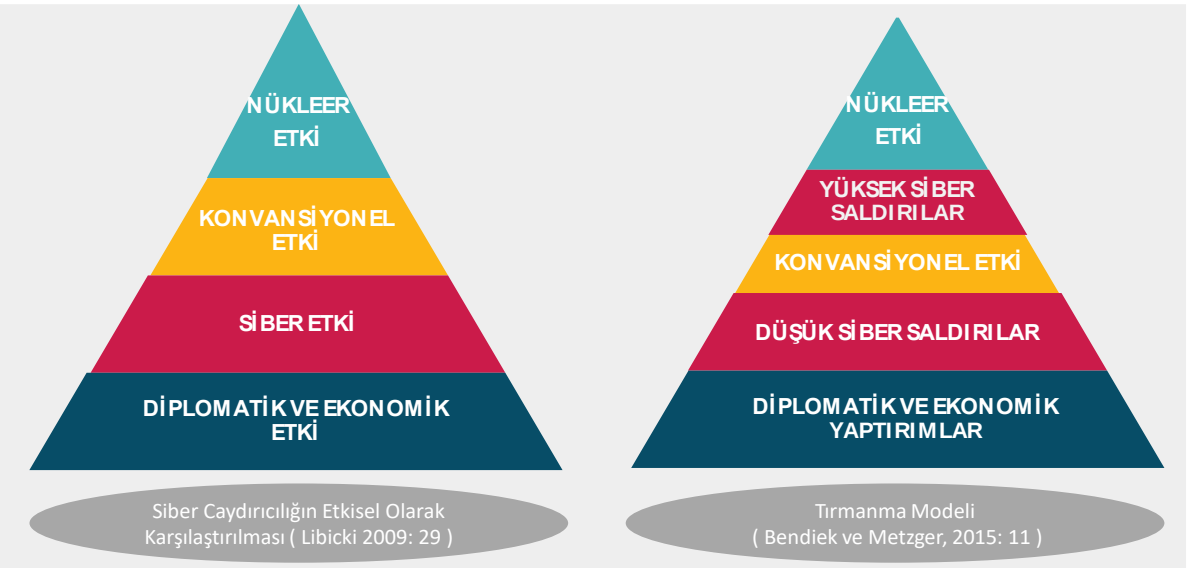
1.3. Siber Savaş

Siber saldırılar ile siber ortamda bulunan donanımlar ve altyapılar hedef alınarak çok ciddi oranda kaşısındakine zarar verebilmek mümkündür. Bu kapsamda uluslararası devletler ile bu alanda bulunan diğer bütün örgütler için coğrafi sınırların önemini neredeyse yok eden siber saldırılar ciddi tehdit oluşturmaktadır. Siber savaşı tanımlamadan önce savaş kavramı üzerinde durulmasında fayda görülmektedir. Savaş uluslararası örgütlerce tanınmış ulus veya

uluslarası devletler aralarında büyük ölçekli çatışmaları olarak değerlendirebilir. Bu kapsamda siber savaş ise bir devletin diğer bir devlet ile siber uzay dediğimiz alanlarında birbirlerine verdikleri zararlar olarak tanımlayabiliriz. Bu zararlar çeşitli alt yapıları kullanılamaz hale getirmek, işlevselliğini yok etmek şeklinde olabilir. Siber savaşlar ile konvansiyonel klasik savaş arasındaki farkları daha iyi anlanamak için iki savaş türü arasındaki benzerlik ve farklılıklar tablo halinde gösterilmiştir.

Tablo 1.1. Klasik Savaş ile Siber Savaşlar Arasındaki Farklar

KRİTERLER	KLASİK SAVAŞ	SİBER SAVAŞ
Saldırı Kaynağı	Yapılan saldırının kim tarafından ve nereden yapıldığının tespit edilmesi basittir.	Saldırının nereden ve kim tarafından yapıldığını bulmak oldukça zor hatta bazen hiç bulunamamaktadır.
Hızı	Bir silahın, hava araçlarının, tankın veya savaşa dahil olan diğer sistemlerin hızı oranında hızlıdır.	Işık hızındadır.
Tespiti	Klasik savaş her daim fiziksel etkiler bıraktığından verdiği hasarı tespit etmekte basittir.	Siber savaşta ise hasar tespiti yapmak zor genellikle imkansızdır.
Kullanılan Araçlar	Mermi, bomba, hücum botları, insansız hava araçları, tank, füze ve radarlar vb.	Bilgisayarlar ve bunlarla ilgili donanımsal, yazılımsal özellikler kullanılarak yapılır.
İhtiyaç Duyulan Metaryel	Klasik savaşta kullanılan silah sistemleri çoğunlukla ileri teknoloji gerektirmektedir. Sürekli geliştirilmesi beklenen çalışma gerekmektedir.	Genellikle var olan bir bilgisayarın kullanılması yeterli olacağından ileri bir teknolojiye gerek olmamakla birlikte daha etkili bir zarar verme anlamında ileri teknoloji kullanılabilir.
Maliyeti	Klasik savaşta kullanılan silah sistemlerinin hepsi maliyetlidir.	Çoğunlukla bir saldırı yapabilmek için sadece bir bilgisayar yeterli olabilmektedir bu yüzden maliyeti ucuzdur.



Şekil 1.3. Saldırıların Etkilerinin Yıllara Göre Karşılaştırılması

Şekil 1.3 incelendiğinde, yüksek siber saldırıların yıllar geçtikçe konvensiyonel silahlarla yapılan saldırılardan daha etkili olduğu çeşitli araştırmalar sonucu siber savaşların verdiği zararların etkilerinin tespitiyle bu kanıya varılmıştır.

1.4. Siber Terör

Devletlerin kritik alt yapılarına, o toplumda yaşayan bireylere ve topluma, sınırları içerisindeki mevcut tüm sosyal ekonomik ve kültürel alanlara yönelik saldırılar sadece düşmanca tutum içerisinde olan bir devlet tarafından değil bir terör örgütü tarafından da gerçekleştirilebilir. Bu sebeple öncelikle terörizim kavramına değinecek olursak kişi veya bir grup tarafından toplumda korku iklimi yaratmak için özellikle sivilleri ve hükümetlerin siyasi davranışlarını hedef alan sembolik saldırılar olarak değerlendirebiliriz. Siber terörizm ise yine devletleri ve onları yöneten hükümet organlarını toplumun gözünde itibarsızlaştırmak için siber ortamda yapılan terörist saldırılar olarak tanımlanabilir. Terörist gruplar siber ortamın alanının çok çeşitli olması ve siber alandaki yapılan saldırıların faillerinin tespitinin zor olmasından istifa ederek son dönemde bu alana daha çok yönelmişlerdir. Yapılacak olan bir terör saldırısının konvasiyonel silahlar veya bombalarla yapılmasının maliyetleri ve riskleri göz önüne alındığında basit bir teknolojik alt yapı ile çok uzak mesafelerden yapılacak olan terör saldırıları terör grupları için vazgeçilmez bir alan olarak ortaya çıkmıştır.

1.5. Siber Güvenlik

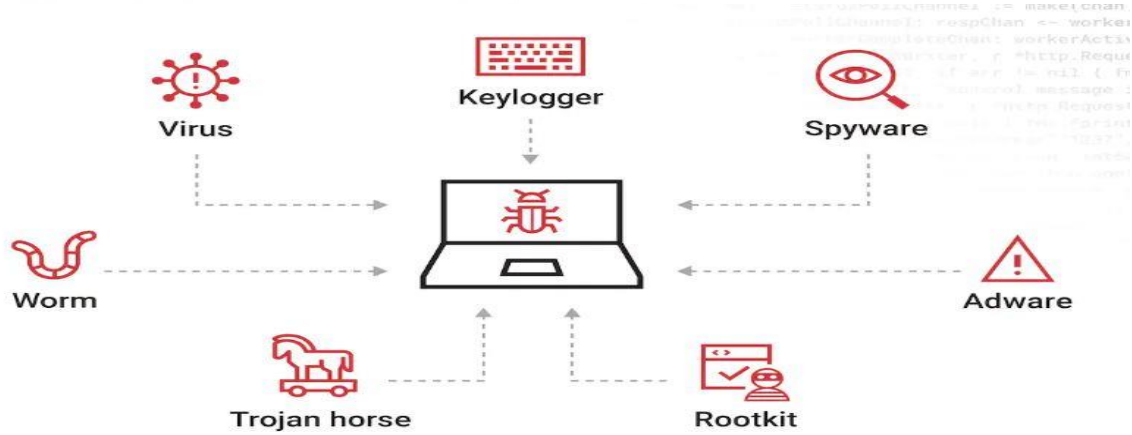
Devletler, devletlerin içerisindeki örgütsel yapılar, kurumlar, şirketler ve o devletin vatandaşları kendilerine yönelecek olan her türlü tehdite karşı elbette bir güvenlik önlemi

almak durumda kalır. Bu sebeple siber saldırılara karşı da devletler hem kendi kurum ve kuruluşlarını hemde vatandaşlarını korumak için siber güvenlik uzmanları yetiştirir ve çeşitli yazılımlar geliştirerek riskleri en aza indirmeye çalışır. Siber güvenlik siber uzay alanını oluşturan bilişim sistemlerinin siber saldırılardan korunmasıdır. Bir başka ifade ile siber ortam içerisinde işlenen bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunması, siber saldırıların tespit edilmesi, bu değerlendirilen ve bulunan tespitlere karşı savunma mekanizmalarının devreye alınması ilişkin faaliyetler bütünü olarak tanımlayabiliriz (Ulaştırma Bakanlığı Eylem Planı, 2020, s.10).

2.BÖLÜM
SİBER SALDIRI TÜRLERİ VE YÖNTEMLERİ

Siber uzay alanında, birden fazla saldırı çeşidi bulunmakta olup saldırı çeşitleri ve buna bağlı olarak güncellenen güvenlik önlemleri ile bu alana yeni saldırı türleri ve yöntemleri eklenmektedir. Bu sebeple aşağıda başlıklar halinde vereceğimiz saldırı türleri, hangi tür sistemler üzerinde hangi araçların kullanılarak siber saldırıların yapıldığı genel olarak izah etmektedir. Tezin amaçladığı hususlar bağlamında siber saldırı çeşitleri incelenirken siber savaş alanı olarak değerlendirilen özellikle uluslararası boyuttaki saldırılarda kullanılan tür ve yöntemler aşağıda belirtilmiştir.

2.1. Kötü Niyetli Yazılımlar (Malvare)



Şekil 2.1. Kötü niyetli yazılımlara ilişkin görsel, Kaynak: https://l24.im/xdAvq

Kötü niyetli yazılımlar bazen bilmeyerek bazen de tarafımıza gelen bir mail veya sms üzerine ilgimizi çekip tıkladığımız anda telefonumuza, bilgisayarımıza veya devletlerin kritik alt yapılarına erişip zarar veren yazılım türlerindendir. Kötü niyetli yazılımlar biz kullanıcıların haberi olmaksızın telefonlara veya bigisayarlara sızarak zarar vermek amacıyla kodlanmış yazılımlardır. Şekil 2.1 de kötü niyetli yazılımların en önemli türleri gösterilmiş olup aşağıda detaylarına yer verilmiştir.

2.1.1. Virüsler

Virüsler kendisini programların içerisine kopyalayarak, program çalıştığı zaman aktif hale gelen ve kendini tekrar eden girdiği sistemi kullanılamaz hale getirmeyi amaçlayan kod parçalarıdır. Temel amacı yayılmak olan virüslerin aşağıda tanımlanan solucandan (worm) farkı insan müdahalesine ihtiyaç duymasıdır. Genel olarak içerisine gizlenmiş olduğu programı çalıştıran ya da bulunduğu sistem içerisindeki bir aksiyonun insan etkisi ile faaliyete

geçmesiyle birlikte yayılmaya ya da çalışmaya başlarlar. Bazı virüsler ise kendini kopyalamak için sistemin bağlı olduğu yerel ağları kullanabileceği gibi kimisi flash bellek gibi harici depolama araçlarında kullanabilmektedir (Keleştemur, 2015; 222).

2.1.2. Solucanlar (Worm)

Solucanlar veya kurtlar olarak tarif edilen bu yazılımlar kendi başlarına bağımsız bir program olarak görev yaparlar. Kendi kendilerine çoğalabilen ve bir bilgisayardan diğer bilgisayara kendini kopyalayabilen bu zararlı programlar genelde bir network sistemi içerisinde yayılırlar. Virüslerden farkı ise diğer programlara sıçramaması ve herhangi bir insan etkisine ihtiyaç duymamalarıdır. Solucanlar bulundukları bilgisayarda ya da sistemde çoğalarak sistemin diğer sistemler veya bilgisayarla olan bağlantısını koparabilir. Örneğin bir elektrik dağıtım şirketinin veya bir bankanın şubeleri ile olan iletişimi kesebilir (Mutlu GÖLÇELEN 2002; 38)

Bilinen en popüler solucanlara değinecek olursak, Conficker, Stuxnet, Duqu ve Weclhia örnek verilebilir. Microsoft işletim sistemine hedef alan Conficker adlı solucan 2008 yılında tespit edilmiştir. Bu solucan aslında sisteme girmek için bir şifre çözme programı olarak çalışmıştır. Yani Windows sisteminde oturum açmak için kendi içerisinde kayıtlı bulunan binlerce sözcüğü parola olarak girerek sisteme erişmeye çalışmış ve işletim sistemi yöneticilerinden birinin hesabına ulaşarak sisteme dahil olmuştur. Bu saldırıya "sözlük saldırısı (dictionary attacks)" da denilmektedir. Conficker solucanı dünya çapında milyonlarca bilgisayara kendini kopyalayarak en fazla bilgisayara bulaşan solucan ünvanını kazanmıştır. Bu virüs 29 Eylül 2009 tarihinde Atatürk Havalimanındaki sistemlere de bulaşmasıyla bilet ve bagaj işlemleri iletişim kopukluğu sebebiyle manuel olarak yapılmak zorunda kalınmıştır. (Hasan Çiftçi 2013;168)

2.1.3. Truva atı (Trojan)

Truva atı adını taşıyan mekanizma aslında bir programın veya bir oyunun içerisine gizlenmiş parçalı bir koddur. Aslında iyi ve faydalı bir program gibi görüp internet üzerinden indirmiş olduğumuz ücretsiz bir yazılım bazen içerisinde truva atı (trojen) denilen kötü bir yazılım barındırır. Bazen reklam olarak bazen de mail olarak karşımıza çıkan bu faydalı gibi görünen programları indirip çalıştırdığımızda aktif hale gelirler. Daha sonra sistemde güvenlik önlemi ve antivirüs programı olmadığında sistemin host ve serverler hakkındaki bilgilerini ele geçirerek uzaktan erişim ile karşı tarafta bulunan bilgisayara aktarım yaparlar. Böylece bilgisayarınız veya telefonunuz bir başka kişi tarafından yönlendirilmeye açılmış olur. Sisteme giren bu yazılım sayesinde tüm bilgileriniz çalınabilir ve yapmış olduğum tüm şifreli işlemler kaydedilerek karşı tarafa aktarılabilir (ÇÖLGEÇEN 2002; 39).

Tüm bilgilerinize erişebilen bu zararlı yazılımlar tarihte anlatıldığı üzere Odysseus'un truva surlarını geçmek ve şehri ele geçirmek için yaptırmış olduğu tahta atdan ismini alır. Kendilerine tanrının hediyesi olduğunu düşünen şehir sakinleri bu tahtadan atı içeri aldıktan sonra gece geç saatlerde bu atın içinde saklanan askerler bulundukları yerden çıkıp kale kapılarını açmış ve şehrin ele geçirilmesinde büyük rol oynamıştır. Yani yararlı gibi görünür hatta bazen işinize de yarayan bir program olarak karşınıza çıkar. Sizin birtakım ihtiyaçlarınızı karşılar gibi görünürken geri planda zararlı işlemler yapar casus bir yazılım gibi kullanılabilir.

2.1.4. Çeşitli zararlı yazılımlar

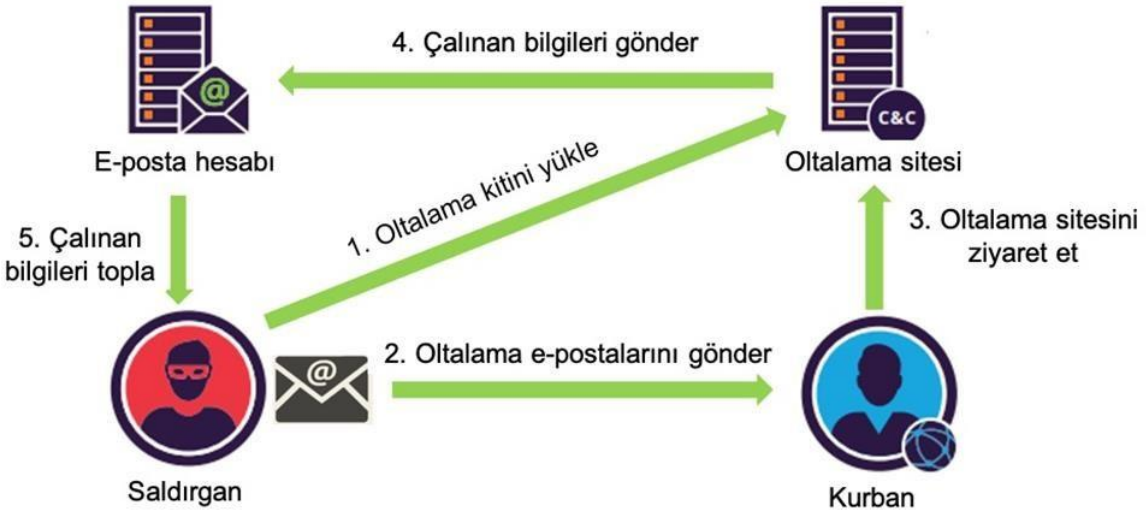
Yukarıda zikredilen virüs, solucan ve truva atları kadar göz önünde olmasa da yine birbirinden bazı özellikleri nedeniyle ayrışan çeşitli zararlı yazılımlar bulunmaktadır. Örneğin rookit adı verilen zararlı yazılımlar bilgisayara girdiği zaman bilgisayardaki görmek istediğiniz bilgilerin görünmemesini sağlarlar. Genellikle işletim sistemine entegre olurlar ve bu rootkitleri bulup temizlemek bir hayli zorlaşır. Keylogger ise adından anlaşılacağı üzere hangi tuşlara basıldığını kaydedip diğer taraftaki saldırgana ulaştıran kötü niyetli yazılımlardır. Bu sayede hangi sayıların girildiğine bakılarak şifreler çözülebilmektedir.

Mantık Bombası (logic bomb) diye adlandırılan zararlı programlar ise bilgisayara sızdığında zaman ve mantıksal bir duruma göre harekete geçen yazılımlardır. Yani bu zararlı yazılımı gönderen kişi bilgisayarın zararlı yazılıma kodlanan bir programı veya bir işlemi kullanıcı tarafından yapmaya başladığı ana kadar sistemde kendini gizleyebilir. Bu yönüyle truva atına da benzerler. Yazılım bir saatli bomba gibi belli bir saati veya zamanı bekleyerek bulunduğu sisteme zarar verebilme ve sistemi yok etme yeteneğine sahiptir.

Ransomware adlı fidye yazılımı ise şantaj yazılımı olarak da adlandırılır. Bu yazılımlar sayesinde fidye talebinde bulunmak için bulaştığı bilişim sistemleri üzerindeki dosyaları kendi sistemi ile şifreleyerek asıl kullanıcının bilgisayarı açmasına engel olur. Bu yazılımlar da genellikle anonim olması için bitcoin yoluyla fidye talep edilir.

2.2. Oltalamalar (Phishing)

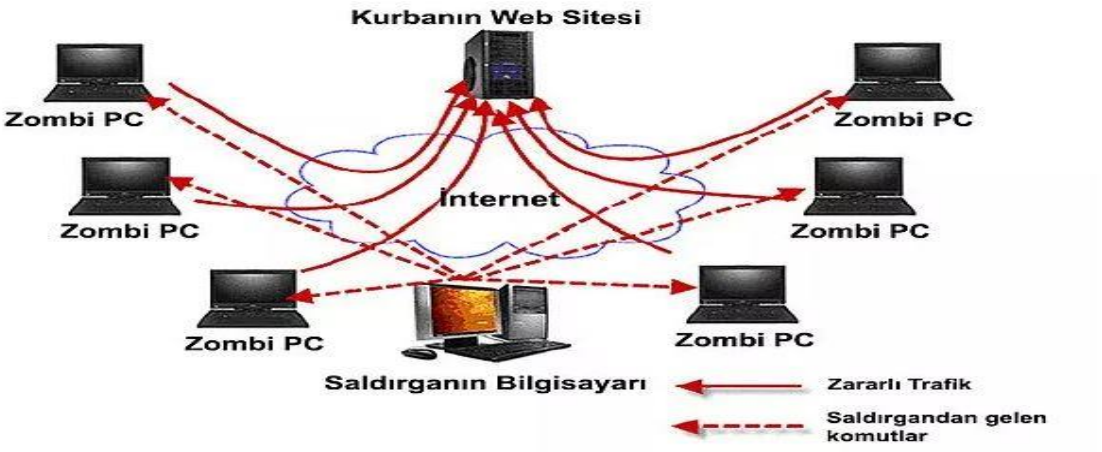
Genellikle maddi bir kazanç elde etmek için kişileri veya şirketleri dolandıran siber saldırı türüdür. Bu yöntem ile bilişim sistemi kullanıcılarının kişisel bilgilerine, kredi kartı bilgilerine ve buna benzer tüm kişisel alanına çeşitli siber saldırı araçları kullanılarak yapılan saldırı ile saldırganların menfaat elde ettiği yöntemdir. Bu yöntemde genelde elektronik posta yolu veya web sayfaları kullanılarak şahıslar veya şirketler mağdur edilmektedir. Dolandırıcılar sanki kullanmış olduğu bir bankanın ara yüzüymüş gibi sitelere girmesini sağlayarak, bazı sitelere reklam şeklinde sızarak ya da mağdura bir e posta göndererek tuzağa düşmesini beklerler.



Şekil 2.2. Oltalama saldırılarını anlatan görsel Kaynak: https://l24.im/Ri68TO

Bu süreç yukarıda şekil 2.2 görsellerle desteklenerek anlatılmıştır. Öncelikle mağdurda kendisine gönderilen bir e-postaya tıklaması ve resmi bir siteye veya kuruma yönlendirildiği algısı oluşturulur. Daha sonra ise mağdurun kişisel bilgilerini sisteme girmesi ile veriler çalınır ve bu verilerin kredi kartı bilgileri olma ihtimali düşünüldüğünde zararların ne denli yüksek olacağı açıktır. Linkte yazılan talimatları uygulayan mağdurun girmiş olduğu bilgiler aslında bir banka sitesinin aynı ara yüzü gibi görünse de yeme düşen balık misali mağdur saldırganın kancasına takılmış olmaktadır. Bu oltalama yöntemine maillerimize düşen spam adı verilen bazı reklam içerikli gereksiz e-postalar aracılık etmektedir.

2.3. BotNet ve Zombi BilgisayarlarÜlkelerin birbirlerine karşı yapmış olduğu saldırıların bir kısmında bu saldırı türü kullanılmaktadır. Şöyle ki saldırgan uzaktan çeşitli saldırı araçları ile ele geçirmiş olduğu bilgisayarı kontrol ederek istediği amaçları yerine gitmek için bazen toplu halde bazen de ferdi olarak bir kuruma veya siteye yoğunluk oluşturarak sitenin kilitlenmesine kullanılamaz hale gelmesine sebep olur. Bu durum aşağıda şekil 2.3 de gösterilmiştir.

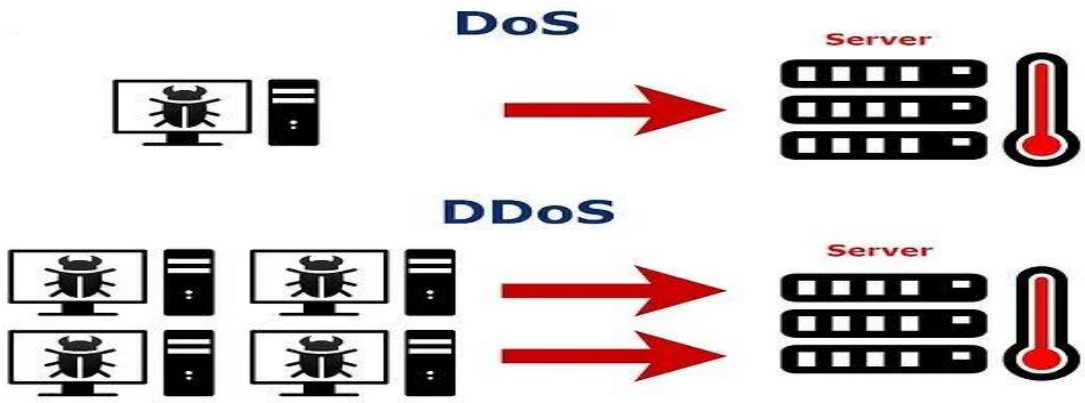


Şekil 2.3. Botnet Saldırısını anlatan görsel, Kaynak: https://l24.im/SXHdza

Zombi bilgisayar bir başka ifade ile köle bilgisayar olarak da adlandırılmaktadır. Hedefteki sisteme sinsice yüklenen uygulamalar, sistem üzerinde nasıl bir faaliyetler yapacağı belirlendikten sonra harekete geçerler. Bu bilgisayarlardaki kötücül yazılımlara veya uygulamara ise bot adı verilmektedir. Kullanıcılarının hiçbir şeyden haberi olmadan, saldırıyı yapanlar tarafından kontrol edilen bu cihazlar, botlar sayesinde birer saldırı makinesine dönüşmektedir. Botlar, yazılan kodlara göre otomatik faaliyete geçen ve birtakım yönetimsel araçları ele geçiren bilgisayar yazılımlardır. Yani kullanmış olduğunuz bilişim sistemine sızmış bir bot varsa bilgisayarınız bir bilgisayar korsanına hizmet ediyor olabilir (Hasan Çiftçi 2013;154).

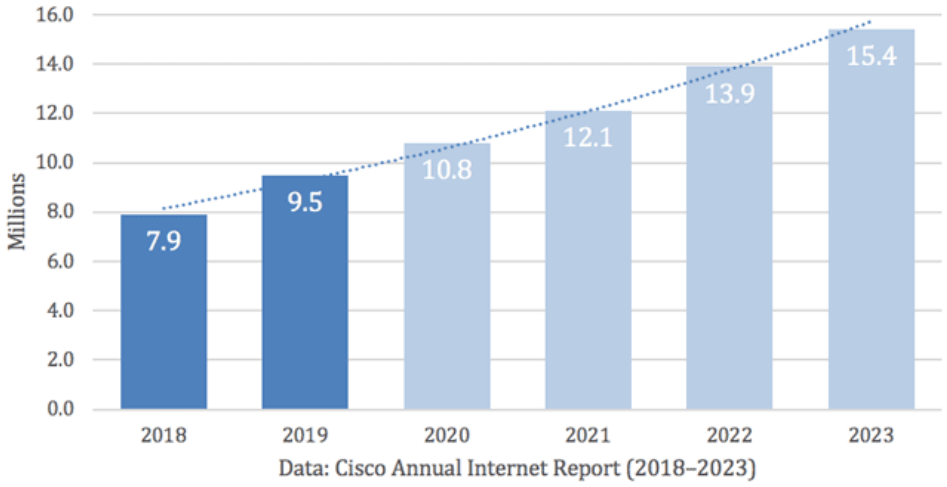
2.4. Hizmeti Engelleme (Dos/DDoS) Saldırıları

DDoS saldırısı (Disributed Denial-of-Service) internete bağlı olan bir sistemin hizmetlerinin geçici veya süresiz olarak aksatılarak, bir makineye veya ağ kaynaklarına asıl kullanıcılar tarafından ulaşılamamasını amaçlayan bir siber saldırıdır. Bu durumu izah eden görsel aşağıda şekil 2.4.1' de gösterilmiştir.



Şekil 2.4. Dos/DDos saldırını anlatan görsel, Kaynak: https://l24.im/eXRrZlB

DDoS saldırıları sonrası, saldırı yapılan kurum örneğin bir banka ise internet sayfası, mobil uygulaması, ATM ve POS cihazları vatandaşa hizmet veremez hale gelir. Bunun yanı sıra, bankanın hizmet aldığı internet sağlayıcısı da saldırılardan etkileneceği için banka da kendi alt yapısına ulaşamayabilir. Saldırganlar, özellikle IP adreslerini gizleyerek, saldırının gücünü arttırmak için "IP Spoofing" yöntemiyle saldırı paketinin kaynak IP adresini hedeflerindeki sistemin IP adresi olarak tanımlayıp açık olan sunuculara "TCP SYN-ACK" isteği gönderirler, yansıtıcı olan sunucular da isteğin nerden geldiğine tespit ettikten sonra boyutu daha büyük olan cevapları saldırganların hedefindeki adrese iletmek durumunda kalır. Böylece, yoğun ağ trafiği sebebiyle hedeflenen sistemin kaynakları tükeneceğinden asıl kullanıcıları tarafından erişilemez hale gelmektedirler (Saygılı, 2020, s3).



Şekil 2.4. Cisco Annual İnternet Raporu Kaynak: https://l24.im/CAN5ws

Yukarıda gösterilen (2.5) grafikten anlaşılacağına göre Cisco Annual İnternet Raporunu hazırlayan uzmalar 2018 yılı içerisinde toplamda 7.9 milyona ulaşan Ddos saldırılarının 2023 yılına gelindiğinde 2 katını aşarak 15 milyona ulaşacağını tahmin etmektedir. Bu veriler göz

önüne alındığında ve aşağıda örneklerine yer verilen saldırılara bakıldığında Ddos saldırılarının son dönemde ciddi artış gösterdiği ortadadır.

2.5. Sosyal Mühendislik Faliyetleri

Siber saldırıların en önemli özelliklerinden biri kuşkusuz karşı tarafı bir şekilde aldatmaktır. Bunu başarabilmenin yolu ise karşı tarafı etkileyerek yaptırmak istediğini onun eliyle kolayca yapabilmektir. İnsanların psikolojileri ve davranışlarını kullandıkları progralar ile çok iyi tespit edebilen saldırganlar, yapmış oldukları tespit sonrası çözümledikleri bir insan topluluğunu bir kurum veya siyasal bir sisteme karşı harekete geçirmeye yönlendirebilirler. Bunu yaparken kendini de o gruptan biri gibi tanıtan saldırgan kişinin tanıdığı bir ismin yerine geçerek sanki onu temsil ediyor gibi hareket edip yönlendirme yapmaktadır. Örneğin 2010 yılında başlayan "Arap Baharı" ve 2013 yılında ülkemizde yaşanan gezi olaylarında, sosyal medya hesapları çalınan kimi ünlü hesaplar üzerinden insanlar galeyana getirilerek kendi amaçlarına hizmet etmek için yönlendirilmiştir. Bu yaşanan hadiselere siber saldırıların siyasi, toplumsal ve medya yönünün etkilerinde detaylı olarak değinilecektir.

3.BÖLÜM
SİBER SAVAŞLAR VE ETKİLERİ

Siber savaşlar genel olarak ülkelerin siber güçleri ile siber ortamlarda gerçekleştirdikleri mücadelelerinin ortak adıdır. Bir siber saldırının siber savaşa dönüşmesi saldırıya uğrayan ulus devletin bunu ulusal güvenliğine saldırı olarak nitelendirip savunma yapması veya karşı saldırı gerçekleştirmesine bağlıdır.
Siber saldırıların ilk örneklerinin ise Rusya'nın 1982 yılında Kanadalı bir şirketten istihbarat faaliyeti olarak çaldığı bir yazılımı fark eden ABD'nin bu yazılıma trojan virüsünü eklemesi ile ortaya çıkmıştır.

Siber savaşların ilk izlerine 1990 yılında ABD'nin Körfez Savaşında, o tarihe kadar dünyanın kara orduları içerisinde 5. büyük ordusu olan Irak ordusunun, ağır bir darbe almasında rastlarız. Telsiz frekans tespit sistemleri üzerinden ırak ordusunun tüm iletişim ve görüşme trafiğini ele geçiren ABD'ye karşı birlikleri arasında çeşitli iletişim yolları izlemeye çalışmıştır. Sivil tır şoförleri üzerinden yazılı bilgiler göndermeye çalışan Irak ordusundaki iletişim zafiyeti beraberinde hezimetle sonuçlanmıştır (Mitnick & Simon, 2013).

Bu saldırılarla ilgili detaylı bir inceleme yapıldığında;

Tablo 3.1. 1990-2022 Yılları Arası Yapılan Siber Saldırılar Kronolojik olarak sıralanmıştır.

	Tarih	**Saldırı Adı**
1	1990	Körfez Savaşı
2	1998	ABD'nin askeri üslerine ve NASA'ya yapılan Ay Işığı Labirenti Saldırısı
3	1999	Çin Büyükelçiliğinin Bombalanması Sonrası Yapılan Saldırı
4	1999	Nato-Kosova krizi
5	2001	Avustralya Atık Sistemi Scada Vakası
6	2001	Code Red Vakası
7	2001	ÇİN - ABD arasında yaşanan siber saldırılar (Hainan Adaso Olayı)
8	2003	ABD tarafından 2. Kez Irak işgali zamanında siber saldırıları
9	2003	Titan Rain Vakası (2002-2006 yıllarını kapsayan)
10	2003	ABD ve Kanada Elektrik Kesintisi (scada)

11	2007	Estonya Vakası
12	2007	Suriye-İsrail Gerginliği
13	2008	Rusya – Gürcistan Vakası
14	2008	İsrail – Filistin Gerginliği
15	2009	JSF- F35 Uçağı Verilerinin Çalınması
16	2010	Stuxnet Vakası
17	2010	Mavi Marmara Saldırısı
18	2010	Tunus Olayları-Arap Baharı
19	2011	ABD İnsansız Hava Araçları Filosuna Yapılan Saldırı
20	2012	Redhack – Anonymous – Türkiye Saldırısı
21	2013	OpIsrael Operasyonu
22	2013	Edward Joseph Snowden Wikileaks Olayı
23	2016	ABD-Çin-Rusya Siber Savaşı
24	2021	JBS SA'ya Siber Saldırı
25	2021	ABD Colonial Pipeline Petrol Boru Hattı Saldırısı,
26	2021	İran Natanz Nükleer Santraline Saldırı
27	2022	Arnavutluk – İran Gerginliği
28	2022	Rusya- Ukrayna Savaşı

Yukarıda 1990 yılından 2022 yılına kadar ki dönemde yapılmış olan ve tespit edilebilen uluslararası siber saldıralar (Tablo 3.1) listelenmiştir. Tüm bu saldırılar detaylı bir şekilde incelendiğinde bazı saldırıların ekonomik boyutunun ne kadar ciddi sonuçlara yol açtığı, bazılarının ise ekonomik zararından ziyade ülkelerin siyasi yapılarını değiştirecek düzeyde etkili olduğu görülmüştür. Yukarıda tez çalışması kapsamında yapılan araştırma kapsamında devletler arası boyut kazandığı gözlemlenen siber saldıra yer verilmiştir. Uluslararası boyut kazanmayan ancak çok ciddi ekonomik, siyasi, toplumsal ve mali sonuçları olan bir kısım saldırılara ise saldırıların etkileri başlığı altında yine yer verilmiştir. Aşağıda örneklem analiz yöntemi kullanılarak yukarıda listelenen siber saldırıların ülkelerin ekonomilerine, siyasetine, toplumsal yaşamına ve medya üzerinden etkilerine değinilecektir. Bu etkilere değinmeden hemen önce listenen saldırılar hakkında kısa bilgiler verilecektir.

3.1. Örnek Olaylar

Geçmişten bugüne siber savaşlar olarak değerlendirilen olaylar kronolojik sıralamaya göre yukarıda belirtilmiş olup temizin bu bölümde ise küresel çapta meydana gelmiş siber saldırı vakalarına ve bu saldırıların örnek olaylardaki yaptığı etkilere değinilecektir.

3.1.1. Körfez savaşı

1990 yılında Amerika Birleşik Devletleri öncülüğündeki koalisyon ile Irak Devleti arasında yaşanmış olan Körfez Savaşında (Şekil 3.1.) o dönem için dünyanın 5. Büyük kara ordusu gücüne sahip olan Irak bugünün bilgisayar sistemlerine bağlı siber internet saldırıları yaşamasa da yine siber saldırılar olarak değerlendirilen telekomünikasyon sistemlerinde yaşadığı sıkıntı yüzünden savaşı kaybetmiştir.


Irak, Kuveyt'i isgal etti

Irak tankları, Kuveyt'te...
Amerikan gemisi Körfez yolunda

IRAK

KUVEYT

Şekil 3.1. Irak'ın Kuveyti işgalini anlatan gazete haberi, Kaynak: https://l24.im/SyD

Kulağa basit bir olay gibi gelse de körfez savaşının başlamasına çok kısa bir süre kala ABD Iraka'a ait olan füze bataryaları ve hava savunma sistemlerinin yerini bulmak için geliştirmiş olduğu telsiz frekanslarını tespit edebilen cihazlarını koalisyon ülkelerine yani Irak'a sınırı olan bir kısım devletlere konuşlandırmıştır. Önce telsiz konuşmalarını frekanslara girerek dinleyen daha sonra ise sanki Irak askerlerinin üst komuta birlikleri gibi onlarla aynı frekanslar üzerinden görüşme sağlayıp yanlış bilgilendirmeler yapan ABD bu şekilde Irak ordusunun tüm iletişim düzenini alt üst etmiştir. Irak devleti her ne kadar telsizleri kullanmayıp kablolu sabit

telefonları kulllanmaya çalışsa da koalisyon güçleri yine aynı yöntemlerle bu iletişimi de sabote etmiştir. Irak hükümeti son çare olarak taşımacılık yapan kamyon ve tır şoförleriyle cephe ve cephe hattı için bilgi akışı sağlamaya çalışsada bu öğrenen ABD bu sefer de yük taşımacılığı yapan sivil araçları vurmaya başlamıştır. Neredeyse tüm emir komuta zinciri iflas eden Irak ordusu bu haliyle savaşa devam edememiş 4 gün içerisinde anlaşma imzalamıştır (Mitnick ve Simon, 2013, s.288-289)

3.1.2. ABD'nin askeri üslerine ve NASA'ya yapılan saldırı

ABD tarihindeki en büyük siber saldırıyı 1999 yaşamıştır. Yaşanan bu olayda enerji bakanlığı, Pentagon ve NASA'nın gizli verileri çalınmıştır (Aşağıda şekil 3.2. de olaya ilişkin gazete manşetine yer verilmiştir)


The first article that mentioned "Moonlight Maze" appeared on 25 July 1999, The Sunday Times, London

THE SUNDAY TIMES · 25 JULY 1999

OPERATION MOONLIGHT MAZE

Missing secrets

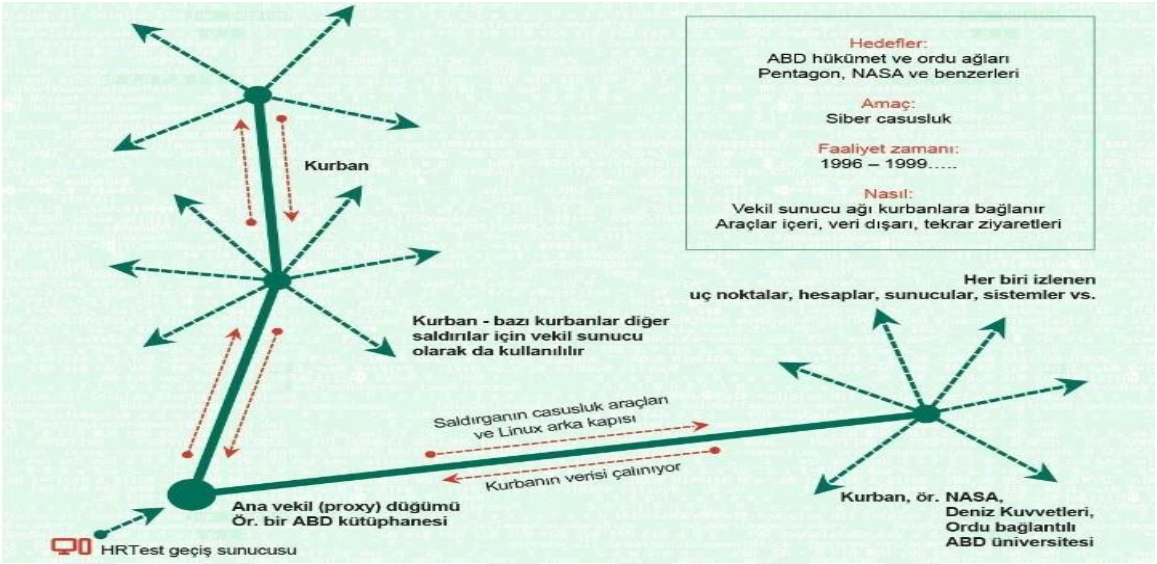
Russian hackers steal US weapons secrets

by Matthew Campbell Washington

Şekil 3.2. Rusyanın saldırını gösteren haber yazısı, Kaynak:

Saldırı ile askeri birliklerin bulunduğu yerlerin konum bilgileri, stratejik araştırma faaliyetleri, uzaya alanında yapılan bir kısım gizli çalışmalar ve ülke savunmasında kullanılan silahların teknolojileri Rusya üzerindeki bir servis sağlayıcı üzerinden çalınmıştır. Bu saldırının yapılış şekli bir güvenlik şirketi olan Kaspersky tarafından çizilmiş olan aşağıdaki resimde (Şekil 3.2) görüldüğü üzere tarif edilmeye çalışılmıştır. O güne kadar edinilmiş olan stratejik bilgiler bir anda el değiştirerek Rusya'nın eline geçmiştir. Saldırının ekonomik boyutunun ne kadar büyük olduğu çalınan verilerin değeri ile orantılı olup bir ülkenin en ödemli sırlarının bir başka ülkeye geçtiği düşünüldüğünde tarif edilemez boyutta olduğu açıktır.[1]

[1] Ayrıca saldırının metodu ile ilgili detaylı bilgi için https://www.youtube.com/watch?v=9RorL9y70GU



Şekil 3.3 Kaynak: 2017 Yılı Kaspersky Lab. Tarafından hazırlanmıştır

O güne kadar edinilmiş olan stratejik bilgiler bir anda el değiştirerek Rusya'nın eline geçmiştir. Saldırının ekonomik boyutunun ne kadar büyük olduğu çalınan verilerin değeri ile orantılı olup bir ülkenin en ödemli sırlarının bir başka ülkeye geçtiği düşünüldüğünde tarif edilemez boyutta olduğu açıktır.

3.1.3 Çin büyükelçiliğinin bombalanması sonrası yapılan saldırı

1999 yılında Natonun bir tatbikatı sırasında Belgrad'daki Çin'in büyükelçilik binası yanlışlıkla vurulmuştur. Bundan çok kısa bir süre sonra kendilerine Çin Kızıl Korsanlar Birliği diyen grup ABD'ye ait olan bir çok web sitesine saldırılar düzenlemiştir. ("Honker Union", ,2009)

3.1.4 Nato/Kosova krizi

Yugoslavya'nın dağılma sürecinde Kosova Kurtuluş Ordusuna NATO müdahale etmiştir. NATO uçaklarının Sırbistan'ı bombalaması üzerine "Black Hand" isimli Sırp yanlısı olan ve Batı karşıtlığı ile bilinen hacker grupları NATO'nun resmi sitelerine ve internet altyapısına saldırmıştır. Bu saldırılar ile, NATO'nun askeri operasyonlarının engellenmesi veya bozmaya çalışıldığı düşünülmektedir. "Black Hand" adlı hacker grubu ismini, 1. Dünya Savaşı'nın başlamasına neden olan Pan-Slav gizli bir topluluktan almıştır. Savaş esnasında "Black Hand" adlı hacker grubunun NATO'nun karargahındaki en önemli bilgisayarları ele geçirip, tüm verileri sildiği iddia edilmiştir. (Arquilla, 2001 sy. 240-248) Kosova Savaşı, NATO örgütünün karşılaşmış olduğu ilk siber savaş olayıdır. Çatışmalarda ABD uçaklarının Belgrad'ta bulunan Çin Büyükelçiliğini yanlışlıkla bombalamasıyla, Çinli hackerler da ABD'ye karşı saldırı

başlatmıştır. NATO'ya yapılan bu saldırı ile web sitelerine bırakılmış olan bildiri mahiyetindeki mesajlar, saldırganların sırplar olduğunu göstermektedir. Nato yaşanan bu olaydan sonra siber güvenlik kapsamında ilk önlemlerini almaya başlamıştır.

3.1.5 Avustralya atık sistemi scada vakası

Atık depolama sistemine yapılacak olan bir saldırının ilk etepta tahribat değerinin çok yüksek olmayacağı düşünülse de 2001 yılında Avustralya da gerçekleşen olay sonrası herhangi bir sisteme yapılan saldırının yan kolları ile birlikte çok büyük hasarlar verebileceği anlaşılmıştır. Şöyle ki yazılım geliştirme ekibinden olan bir çalışan şirketin otoparkından wifi ile bağlanarak yaklaşık 46 kez sistemi hackleyerek 264.000 galon ham lağım atığını nehirlere bırakmıştır. Sistemin çalışmadığı süre ve pis atığın nehirlere girmesi sonrası ciddi anlamda ekonomik kayıp yaşanmıştır. Yaşanan kötü koku nedeniyle nehir çevresindeki parklar ve piknik alanları uzun süre kullanılamamış ülkenin en önemli turistik alanlarına gelen turist sayısı ciddi oranda azalmıştır. Nehirlerde balıkçılık faaliyeti yapıp geçimini sağlayan yüzlerce balıkçı yine atıklar sebebiyle ekosistemin zarar görmesi ve balıkların ölmesi sebebiyle uzun süre işsiz kalmıştır. Atık su sistemi üzerinden elde edilip şehirlere sağlanan elektrik de bir süre yine sisteme verilememiştir.

Şekil 3.4. Atık sisteminin yapısını gösteren görsel, Kaynak: https://l24.im/fFUXc

Yukarıdaki (Şekil 3.4.*)* gösterildiği üzere bir atık sistemi birçok yapının bir araya gelmesi ve sisteme bağlanması ile oluşmaktadır. Bu sisteme yapılan saldırı sonrası sistemin güvenli hale gelebilmesi için Avustralya hükümetinin milyonlarca dolar harcadığı haber kaynaklarına yansımıştır. ("SCADA Incidents",2009)

3.1.6. Code red vakası

2001 yılı temmuz ayı ortalarında tespit edilen Code Red solucanı ABD'de Microsoft'un IIS Web sunucularındaki güvenlik açığından yararlanarak tahmini olarak 300.000 bilgisayara kendisini kopyalamıştır. Solucan bir mantık bombası gibi hareket ederek ayın 1 – 19 arasında kendisini çoğaltıp, 20 – 27 arasında özellikle Beyaz Saray'ın sistemini Hizmet Dışı Bırakma (DOS) saldırısı gerçekleştirmiş, 27'sinden ay sonuna kadar da bilgisayarda hiçbir aktivite yapmadan sessiz bir şekilde kalacak şekilde hazırlanmış ve bu şekilde hareket etmiştir. Dünyanın en büyük şirketlerinden olan Microsoft'un güvenlik açığı vermesi sonrası yapılan saldırılar dünyada geniş yankı uyandırmış ve güvenlik programlarına olan talebi 3-4 kat artırmıştır. Yapılan saldırı ile Beyaz Saray sitesinin ana ekranında "Çinliler Tarafından Hacklendi" yazısı (Şekil 3.5.) bulunması infial oluşturmuş, insanlarda bilgisayarlarının ele geçirilebileceği kaygısını daha da yükseltmiştir. [2]

Şekil 3.5. Saldırı sonrasına ait görsel, Kaynak: https://l24.im/NzT5

Saldırı sonrası dünya çağında internet hızlarında ve sitelere erişimde ciddi oranda yavaşlama yaşanmıştır. Bu saldırının Amerikan kamuoyuna mesaj vermek için yapıldığı basında geniş yer bulmuştur.

[2] Bkz. Saldırının detayları ve oluşum aşamaları için https://www.kaspersky.com.tr/blog/history-lessons-code-red/10909/ sistesini ziyaret edebilirsiniz.

3.1.7 Çin/ABD siber saldırısı (Hainan adası olayı)

Güney Çin Denizi açıklarında bir ABD casus uçağı (Şekil 3.6*)* ile bir Çin jetinin çarpışması sonrası 80.000'i aşkın hacker ABD'nin saldırgan tutumunu eleştirdiğini göstermek ve bunun gibi saldırılara karşı savunma yapacaklarını bildirdikleri bir dizi saldırı başlatmıştır.

Şekil 3.6 Olayda adaya düşen ABD uçağının görselidir, Kaynak: https://l24.im/UfGQlq

Deniz yetki alanlarının tartışmalı olduğu bölgede Amerikan casus uçaklarının radar sisteminde görünmemesi ve sonrasında yaşanan kaza siber alandaki teknolojik gelişmelerinde ne kadar önemli olduğunu bir kez daha göstermiştir. Yapılan siber saldırılarda ise genellikle Amerikan Savunma Bakanlığı ve Amerikan Hava Kuvvetleri hedef alınmıştır. ("Hainan Island İncident " 2002)

3.1.8 ABD'nin 2. kez Irak'ı işgalindeki siber saldırılar

2003 yılında ABD ilk körfez savaşında yaptığının neredeyse aynısını yine yaparak bu sefer de Irak makamlarına ait kapalı devre bilgisayarlara sızmıştır. Bu şekilde Irak Savunma Bakanlığı verileri üzerinden on binlerce Iraklı subaya teslim olmalarını istenildiği şekilde mesajlar göndermiştir. Bu hali ile zaten mezhepsel ve etnik temelli saldırılara maruz kalan Irak devletinin bir kısım subayları tek bir kurşun atmadan teslim olmuş ve silah bırakmıştır. Basit bir mesajla askerin moralini bozan veya olandan daha farklı bir algı oluşturan ABD 2. Kez Irak ile karşı karşıya geldiği bu savaşta birkaç tuşla savaşın seyrini değiştirebildiğini tüm dünyaya göstermiştir. (Hasan Çiftçi 2013– Sy. 165)

3.1.9. Titan rain vakası (2002-2006 yıllarını kapsayan)

Titan Rain olayı 2002 yılı ile 2006 yılları arasını konu alan ABD Savunma Bakanlığına Çin tarafından yapılan saldırıların gayri resmi adıdır. Saldırı sonrası bir çok basın ve yayın kuruluşunda saldırının Çin tarafından yapıldığı resmi makamlardan alındığı iddia edilen bilgilere göre ifade edilmiştir(Şekil 3.7).

Şekil 3.7 Olaya ilişkin haber manşeti Kaynak: https://l24.im/pXC0e

Aslında bu saldırılardan sadece savunma bakanlığı değil orduya ait mühendislik komutanlığı, deniz sistem merkezi, NASA, bir kısım askeri firmalar ve bazı ABD kamu kuruluşlarıda etkilenmiştir. ABD tarafından "Titan Rain (Titan Yağmuru)" olarak adlandırılan bu saldırılarda kurum ve şirketlerin açıklarından faydalanılarak tarayıcı bir program gibi görünen truva atı sızıntısı yapılarak bilgisayarların güvenlik sistemleri devre dışı bırakılmaya çalışılmış sonrasında elde edilen bilgiler Tayvan üzerinden Çin'e gönderilmiştir. Bu kapsamda tahmini 20 terebayt verinin ABD 'nin yukarıda ismi zikredilen kurum ve kuruluşlarından çalındığı tahmin edilmektedir.(Thornburgh, 2005)

3.1.10. ABD ve Kanada elektrik kesintisi

14 Ağustos 2003 tarihinde gece saatlerinde gerçekleşmiştir. Yaşanan olay sonrası Kanada'nın Ontario eyaleti ve ABD'nin Ohio, Michigan, Pennsylvania, New York, New Jersey eyaletlerinde yapılan siber saldırı sonrası 4 gün boyunca devam eden ve onarılamayan bir elektrik kesintisi meydana gelmiştir. Aşağıda şekil 3.8 da yaşanan siber saldırı sonrasına ait uydu fotoğrafı görülmektedir.

Şekil 3.8 2003 yılı olay gününü gösteren uydu fotoğrafı, Kaynak: https://l24.im/kWgoeR

Yaklaşık olarak 50 milyon insanın etkilenmiş olduğu kesinti sonrası ABD'ye saldırının maliyeti 30 milyar doları bulmuştur. Kanada'nın da Ontario şehrinde üretimin aksaması sonucu zararın yaklaşık olarak 2,3 milyar Kanada doları olduğu tespit edilmiştir. Yapılan saldırının boyutu çok ciddi olup saldırının Rusya menşeili olduğu tahmin edilmektedir. ("U.S.-Canada Power System", 2005)

3.1.11. Estonya vakası

2007 yılında Nüfusu 400 bin civarı olan Estonya'nın başkenti Tallin'de olan bu vaka Estonya'nın bağımsızlık mücadelesinin parçasını oluşturmuştur. SSCB Nazi işgalinden kurtardığı tüm Doğu Avrupa ülkelerinin meydanlarına büyük Bronz Kızıl Ordu askeri heykelleri (Şekil 3.9) dikmiştir.

Şekil 3.9. Tepki üzerine kaldırılan heykelin görseli, Kaynak: https://l24.im/4nO

Dikilen heykel sonrası Sovyet birliğinin baskısını yıllarca yaşamış olan Estonyalıların tepkisi üzerine heykel kaldırılmıştır. Bu durum Moskova'da farklı bir algı oluşturmuş tam bağımsız Estonya düşüncesi Rus medyasında rahatsızlık oluşturmuştur. Yaşanan heykel kaldırma olayı üzerine Rus siber saldırganlar Estonya'nın web sitelerine ve devletin resmi sitelerine saldırılar düzenleyerek hizmetleri kullanılamaz hale getirmiştir. Bu saldırı dağınık yüzbinlerce bilgisayarın sitelere yönlendirilmesi ile olan bir DSES (Dağınık Servis Engelleme Saldırısı) saldırısıdır. Yani botnet diye tabir ettiğimiz zombi bilgisayarlar aktif hale getirilerek hizmetlerin engellenmesi için kullanılmış ve başarılı olunmuştur. (Clarke -Knake, 2011:13,14)

3.1.12. Suriye-İsrail gerginliği

Suriye devleti İran'ın ve birçok ülkenin yaptığı gibi gizlice nükleer tesis inşasına başlamış ancak bunu enerji üretimi için değil uranyumun uluslararası standartların üzerinde zenginleştirmesi için kullanılmak istediği düşünülmüştür. Bu sebeple de Birleşmiş Milletlerin'in hedef ve ilkelerini ihlal ettiği ifade edilmiştir. Suriye'nin nükleer silah yapmak istediği savını yineleyen İsrail ise tesisin bulunduğu yeri bir gece vurmuştur. Bu saldırıya ilişkin görseller israil kaynakları tarafından yukarıda gösterildiği üzere (Şekil 3.10 basına sızdırılmıştır.

Şekil 3.10. Vurulduğu israil tarfından kabul edilen ve paylaşılan görsel, Kaynak: https://l24.im/mAZaN

Olayın siber saldırı olarak değerlendirilmesi ise tesisi koruyan Rus savunma sistemlerinin gelen saldırıyı hiçbir şekilde görmemesinden kaynaklanmaktadır. Bu saldırıda israil saldırının detayları ile ilgili herhangi bir açıklama yapmazken saldrının bir kaç farklı siber saldırı yöntemi ile yapılmış olabileceği düşünülmektedir. Bunlardan ilki İsrail tarafın bir insansın hava aracını Suriye hava savunma sisteminin radarının bulunduğu yere gönderdiği ancak bir yazılım sayesinde radar sisteminin hava aracını farklı bir nesne olarak algıladığı için aktif hale gelmediğidir. Diğer bir ihtimal ise hava savunma sisteminin içine manuel veya uzaktan bir erişim sağlanarak truva atının yerleştirilmiş olabileceği ihtimalidir. Bu sayede alınan elektronik sinyal olmasına ragmen truva atı virüsü sayesinde bir tuzak kapının sisteme dahil edilerek alınan sinyali bu tuzak kapısından çıkarıp sistemde hiç görünmemiş gibi gösterildiği değerlendirilmiştir. Bununla birlikte sisteme giren bir truva atının içerisinde olan mantık bombasının sisteme boş bir hava sahasını gösterme talimatı verdiği de ihtimaller arasındadır. Sonuç olarak yapılan saldırı sonrası tesis neredeyse işleve başlamadan imha edilmiştir. (Clarke -Knake, 2011:8-11)

3.1.13. Rusya – Gürcistan vakası

2008 yılında Rusya ile Gürcistan arasında yaşanmış olan Güney Osetya Savaşı sırasında Rus saldırganlar Güscistan'a ait olan web sitelerine, ABD ve İngiltere'nin ülkede bulunan büyük elçilik sitelerine saldırılar düzenlemiştir. Hatta Rusya kendi halkına Gürcistanın devlet kurumlarına giriş sistelerinin linkini bir web sitesinde paylaşarak bodnet saldırısı yapılması için talepte bulunmuştur. Rusya üzerinden örneğin bir acil çağrı merkezinin telefon hattının meşgul edilmesine benzeyen bu saldırı aslında basit bir saldırı olarak algılanabilmektedir. Fakat ülkemizde olduğu gibi devlet kurumlarının genel olarak e- devlet uygulamasına

benzeyen elektronik sistemler üzerinden işlemesi süreçlerinde sistemlere ulaşılamaması ülke vatandaşlarını bir hayli zor durumda bırakmaktadır. Gürcistan Rusya üzerinden gelen IP adreslerinin sistemlerine erişimini engellemeye çalışsa da bu seferde Rusya Çin, Türkiye, Kanada gibi ülkelerdeki ele geçirdiği bilgisayarlar üzerinden botnet (zombi bilgisayar) saldırıları yapmıştır. (Hasan Çiftçi 2013– Sy. 167) Gürcistan'a yönelik yapılan siber saldırılardan çıkartılabilecek en önemli sonuç konvensiyonel silahlarla yapılan bir savaşın eş zamanlı olarak siber saldırılarılarla da desteklenmesi ile kısa vadede sonuç alınacağını kanıtlaması olmuştur. Bu saldırılarla birlikte savaş 3 hafta gibi kısa bir sürede Rusyanın lehine olacak şekilde sonuçlanmıştır.

3.1.14 İsrail – Filistin gerginliği

2008 yılı aralık ayında İsrail tarafından özellikle Gazze şeridi boyunca düzenlediği saldırılar sonrası Filistinliler ve onlara destek olan bir kısım hacker tarafından İsrail web sitelerine saldırılar düzenlenmiştir. Bu web sitelerinin ara yüzlerine ve ana sayfalarına İsrail'in aleyhine olan propaganda amaçlı reklamlar ve resimler yerleştirilmiştir. Hackerler İsrail'i yapmış olduğu zulümden bir an önce dönmesi için çeşitli çağrıları bu şekilde hem İsrail kamuoyuna hem de dünyanın başka bölgelerinde yaşayan ancak kendi ülkelerinin sitelerini zaman zaman kullanan savaşa hayır diyen Yahudilere duyurmak için yaptıklarını belirtmişlerdir. Filistinlilerin özellikle Gazze'deki temsilciliğini üstlenen Hamas Filistinli hackerler tarafından 300 İsrail sayfasını (bir banka ve haber sitesi dahil) erişime engelledikleri sosyal medyadan duyurmuştur. Facebook, Twitter ve YouTube gibi kanallar üzerinden sürekli yayınlar yapıp paylaşan Filistinli aktivistler milyonlarca insanın saldırıda ölen sivillerin görüntülerine ulaşmasını sağlayarak kendisi lehine kamuoyu oluşturmayı başarmış gelen tepkiler üzerine İsrail saldırılarını sonlandırmak zorunda kalmıştır. (Varon, 2009)

3.1.15 Jsf- f35 uçağı verilerinin çalınması

2009 yılında gerçekleşmiş olan bu olayda Çin ve Rus hackerlar olduğu iddia edilen bilgisayar korsanları, JSF (Joint Strike Fighter) ucalarını diğer adıyla bugünkü F35 uçakların elektronik sistemlerinin bulunduğu verileri çaldığı biz gazete ile basına sızmıştır. Casusların, uçağın uçuş anındaki bakım sorunlarını tespit eden bir sistem üzerinden birkaç terabaytlık veriyi ele geçirdiğinin tahmin edildiği ifade edilmiştir.2001'de başlayan projenin üretimi 2020li yıllarda bitirilmiştir. Hatta Türkiye de bu uçağın yapımına katkı sağlamış ancak ABD çeşitli bahaneler üreterek uçakları ülkemize teslim etmemiştir. Pentagon'a yaklaşık 1,5 trilyon dolara mal olan bu uçak ABD'nin şimdiye kadarki en pahalı silah sistemidir. Bu sebeple güvenlik seviyesi en üstte tutulan projenin saldırı yapılarak bir kısım bilgilerinin başkalarının eline geçmiş olması büyük bir infiale yol açmış uçakların üretimi uzun süre ertelenmiştir. 2014 yılında yeniden başlanan uçak üretimi bugünlerde devam etmekte olup yaşanan siber saldırı sonrası uzun süre

uçağın üretime alınmaması iddiaları doğrular niteliktedir. Uçağın özellikle yazılım sistemin bir başka kişi tarafından bilinmesi kendisini savunmasız hale getirmektir. Bu sebeple ABD'nin en maliyetli silah sisteminin verilerinin çalışması dünya basınında büyük yankı uyandırmıştır.

3.1.16 Stuxnet vakası

21. yüzyıl içerisinde en ciddi siber saldırı olarak kayıtlara geçen Stuxnet saldırısı, İran'ın Natanz nükleer uranyum zenginleştirme tesislerini hedef almıştır. Stuxnet, ABD ve İsrail tarafından , İran'ın uranyum zengileştirmelerini ve nükleer çalışmalarını akamete uğratmak için kullanmış olduğu ve sisteme soktuğu solucan yazılımdır. Haziran 2010'da varlığı tespit edilebilen virüs İran'ın Natanz ve Buşehr 'daki nükleer tesislerinde ciddi sıkıntı oluşturmuştur. Stuxnet özellikle SCADA (Supervisory Control and Data Acquisition) sistemlerine karşı kullanılmak üzere tasarlanmış, bilinen ilk karmaşık yazılımdır. İran nükleer tesisine girmeyi başarmış olan Stuxnet virüsü, yavaş yavaş sisteme zarar vermeye başlamıştır. Santrifüjler uranyum zenginleştirmede kullanılan ve hızlıca dönen makine sistemidir. Virüsün amacı, Santrifüjlerin kontrolünde kullanılan "Programlanabilir Mantık Denetleyicisi" (PLC: Programmable Logic Controller) kontrol devresini ele geçirmektir. Stuxnet'in USB vasıtasıyla, yerel ağdaki Mantıksal Kontrol Aygıtı'na girdiği sonradan tespit edilmiştir. Bir USB sürücüsü vasıtasıyla sisteme bulaşan bu zararlı yazılım, saldırıyı düzenleyen kişilere hareket serbestliği kazandırmış ve Santrifüjlerin hızlarını bazen azaltmış bazen de olması gerekenden daha fazlaya çıkarmıştır. Bu şekilde çalışan sistem ise yanlış sonuçlar vermeye emekleri heba etmeye başlamıştır. Bu şekilde yaklaşık 1000 Santrifüjü bozan virus nükleer tesisin uzun süre durmasına işvelsiz kalmasına sebep olmuştur. Bu saldırı sonrası iran aylarca nükleer santireldeki santrifüjlerin yeniden yapılması için çalışmış büyük bir ekonomik kayıp yaşamıştır. (Holat, Olcay 2021, 117)

3.1.17 Mavi marmara saldırısı

Şekil 3.11. Saldırıya uğrayan geminin görseli, Kaynak: https://l24.im/9dGmSi

İsrail'in uzun bir süre ambargo uyguladığı Gazze'ye temel ihtiyaç malzemeleri kapsamında yardım ulaştırmak için, birçok farklı millet ile değişik dinlere mensup aktivisler ve yardım gönüllülerini taşıyan gemiler (Şekil 3.11) uluslararası sularda bulunmasına ve seyretmesine rağmen 31 Mayıs 2010 tarihinde İsrail askerlerinin insanlık dışı saldırısına uğramıştır. İsrail'in Gazze'ye uygulamış olduğu deniz abluka bölgesine 64 mil uzakta uluslararası sularda gerçekleştirilen bu saldırı anında geminin dünya ile iletişimini kesilmeye çalışılmış ancak ilk aşamada sürekli frekans değiştiren yardım gönüllülerinin arasında bulunan bilinçli bir kaç gencin yardımı ile saldırının başlamasından sonra dahi bağlantı kurulabilmiştir. Ancak saldırının başladığı anlardan dakikalar sonra gemiden tüm dünyaya yayın yapan uydu frekansı kesilmiştir. İnsanı yardım amaçlı yola çıkan gönüllülerden 9'u İsrail askerlerin silahlı saldırısı sonrası hayatını kaybetmiştir. Saldırının ilk anında frekansların kesilememiş olması sonrası görüntüler tüm dünyaya aktarılmıştır. Aksi halde olayların nasıl gerçekleştiği hiçbir şekilde ispat edilemeyeceğinden İsrail yaşanan olaylarda kendisine saldırıldığından bahsile kamuoyunu kendi yanına çekebilmeyi planlamıştır. Gemide tüm insanalrı alıkoyan, kamera kayıtlarını silen İsrail saldırının görüntülerinin dünyaya servis edilmesinden sonra ilk yapmış olduğu açıklamalardaki askerlerine saldırıda bulunulduğu bunun üzerine ateş açıldığı savından vazgeçmiştir. Bu olay özelllikle Türk vatandaşlarının hayatını kaybetmesi üzerine Türkiye'de ve sonrasında Dünya'da büyük tepki uyandırmıştır. İsrail'in, Gazze şeridine sadece insani yardım götüren gemilere saldırmasına tepki gösteren dünyanın birçok yerinden katılım sağlayan haktivist gruplar İsrail'in çok sayıda resmi ve özel web sitesine saldırı bulunmuştur. İsrail'in uzun süre özür dilememesi üzerine saldırılar artarak devam etmiştir. Türk korsanlarından Akhmenrah da bir basın kuruluşuna yapmış olduğu açıklamada yaşanan olay sonrası 5000 İsrail sitesinin çökertildiğini yapılan yoğun saldırı sonrası İsrail'in Türkiye girişli IP'lere sistemini kapatmak zorunda kaldığını ifade etmiştir. (Günal, 2011) Aynı dönemde İsrail Kamu Güvenlik Bakanlığı Devlet Sitesine yapılan saldrıılar sonucu siteye ve bakanlık sunucularına erişim tamamen durmuştur.

3.1.18. Tunus olayları-Arap baharı

2010 yılında başlamış olan ve Arap birliğine bağlı ülkelerde yaşanan hükûmet karşıtı ayaklanma, protesto, ve silahlı isyanlar sonucu Tunus başta olmak üzere özgürlük ve insan hakkı taleplerinin toplumlarda karşılık bulduğu hareketler olarak değerlendirilen olaylarda yaşanan bir takım ekonomik ve siyasi sıkıntıları kendi lehine çevirmeye çalışan batılı ülkelerin destekleri ile harekete geçen hackerların kısım devlet kurumlarının web sitelerine yapmış olduğu saldırılar sonrası işlevsiz hale gelmesi Tunus ve diğer Arap ülkelerini daha da zor durumda bırakmıştır. Ülkede çeşitli ekonomik ve siyasi sıkıntılar varken sosyal mühendislik saldırıları yapan hacker gruplar sosyal medya ortamında bot bilgisayarlar ve hesaplar kullanarak küçük olayları çok büyük gibi göstermiş insanları sokaklara dökmeyi başarmıştır. Daha sonra ise yine sosyal medya platformları üzerinden insanları galeyana getiren siber saldırganlar halkı çeşitli toplu gösteri merkezlerine yönlendirerek toplu hareket etmelerine ve

birlikte güç oluşturmalarına yardımcı olmuşlardır. Olayların daha da büyümesi sonrası halk isyanları ve silahlı çatışmalar baş göstermiş Tunus da başlayan olaylar Libya ve Mısırla devam etmiş Suriye'de ciddi silahlı çatışmalara dönmüş bu halk isyanlarından Ceyazir, Ürdün ve Yemen gibi ülkelerde ciddi şekilde etkilenmiştir. Tunus devlet başkanı Zeynel Abidin Bin Ali 24 yıldır ülkeyi yönetmesine rağmen ülkeyi terk etmek zorunda kalmış, Mısır 30 yıldır devlet başkanı olan Hüsnü Mübarek görevden ayrılmış, Libya devlet başkanı Muammer Kaddafi ise ülkesinde protestoculara karşı vermiş olduğu mücadeleyi kaybederek memleketi olan Sirte şehrinde yakalanarak isyancılar tarafından öldürülmüştür. Yemen ve Suriye'de ise halen silahlı çatışmalar 10 yılı aşkındır devam etmekte olup milyonlarca insan bu savaşlarda hayatını kaybetmiştir. Bir insanın kendisini Tunus'ta yakması sonrası sosyal medya platformları üzerinden örgütlendirilen gruplar, ülkelerinde ciddi ayaklanmalar gerçekleştirmiş ve bu halk isyanları hükümetlerin sonunu getirmiştir. İsyanların özellikle başlarında devletlerin güvenlik kurumları başta olmak üzere tüm kurumlarına siber saldırılar gerçekleştirerek etkisiz hale getirip protestocuların işini kolaylaştıran Anonymous gibi anonim hacker grupları olayların büyümesinde büyük rol oynamıştır. Olayların başlaması ve kanlı sonuçlarının olması bir kısım çevrelerce Arap halklarının oyuna getirildiği şeklinde yorumlanırken bazı kesimler ise sosyal medya ve hacker grupların halkın uyanışına sebebiyet verdiği ve toplumların özgürlüklerine kavuştuğu şekilde yorumlamıştır. Yaşanan olaylarda Arap toplumlarının kalbi olan Mısırdaki hadiselere bakıldığında bir diktatör olarak gösterilen Hüsnü Mübarek devrilmiş yerine demokratik seçimler ile Muhammed Mursi gelmiş sonrasında ise batının taleplerine cevap vermeyen halk seçtiği başkan bir darbe ile görevden alınarak yerine bir asker geçirilmiştir. Diğer ülkelerin olaylar sonrası demokratik bir düzene geçip geçmediği değerlendirildiğinde neredeyse hiçbir fark olmadığı ortadadır. Bu sebeple yüzleri eskimiş olan devlet başkanları demokrasi ve özgürlük bahanelerinin ardına sığınılarak gönderilmiş yerine yenileri geçmiştir. Bu kapsamda siyasal denklemlere dahi müdahale etme ve etkili olabilme gücü olan siber saldırılar ile dışarıdan hiçbir askeri müdahale olmaksızın ülkelerin yakılıp yıkılabileceği ve kendi istemediği siyasi kişi veya grupları hükümetten alarak başkalarının getirilebileceği savı güç kazanmıştır. Arap dünyasında gelişen olaylar bizce siber devrim veya sosyal medya devrimi olarak da adlandırılabilir. [3]

3.1.19 ABD insansız hava araçları filosuna yapılan saldırı

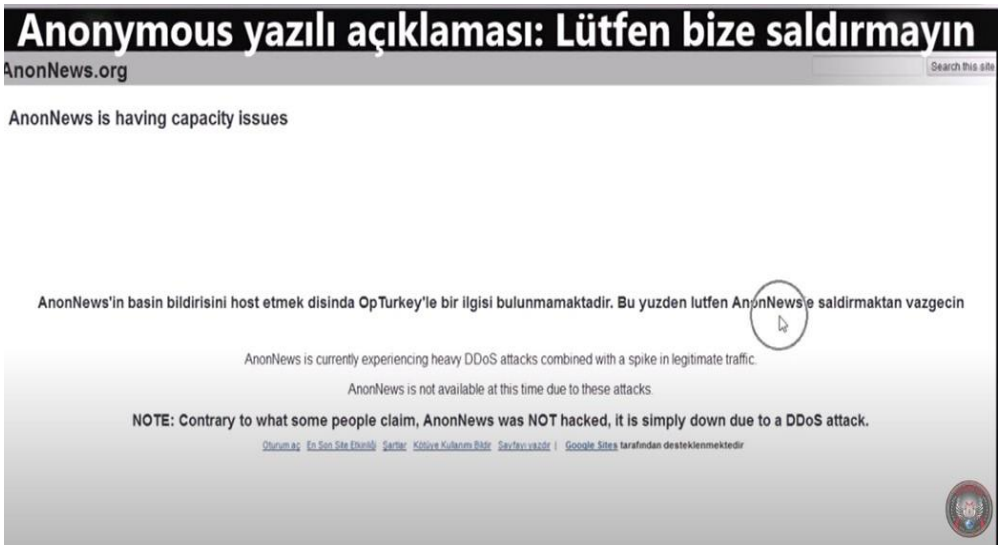
Amerika Birleşik Devletleri gerek Irak'ta ve Yemen de gerekse Afganistan da gerçekleştirmiş olduğu saldırılarında direnişçilere karşı kullanmış olduğu insansız hava araçlarından olan Predatör ve Reaper'ın kontrolünü Nevada Eyaletinde bulunan Creech Hava Üssünden Yapmıştır. 7 Ekim 2011 tarihine gelindiğinde, yukarıda bahsedilen hava üsssünde yer alan ve insansız hava araçlarını control etmekte kullanılan istasyona bilgisayar virüsü bulaştığı tespit

[3] Detaylı bilgi için bakınız: https://tr.wikipedia.org/wiki/Arap_Bahar%C4%B1, Sosyal medyanın etkisi bağlamında Ali Murat Kırık'ın yazısı, detaylı bilgi için https://dergipark.org.tr/tr/download/article-file/59580

edilmiştir. Bu saldırıda her ne kadar insansız hava araçlarının düşmesini veya bir başka noktayı vurmayı sağlayacak ölçüde etkili bir virüs olmadığı saptanmış olup sisteme giren keylogger (tuş kaydedici) virüsünün hava araçları kullanırken hangi tuşlara basıldığını kaydettiği anlaşılmıştır. Her ne kadar bir insansız hava aracını düşürmek veya sistemlerine zarar vermek için bulaşmayan bir virüsün ne amaçla sızdığı tam olarak çözülemesede herhangi bir saldırı için kalkış iha'nın nereye gittiğini ve nereyi vurabileceğini basılan tuşlar ve girilen kodlardan tahmin etmekte ciddi bir istihbarat faaliyeti olarak öne çıkmaktadır. (Hasan Çiftçi 2013– Sy. 178)

3.1.20 Redhack/Anonymous/ Türkiye saldırısı

Anonymous kelime anlamı anonim olan bir hacker topluluğudur. Topluluk dünyanın farklı bölgelerinden insanların kimliklerinin gizli tutulduğu internetteki özgürlükleri ve ifade haklarını savunduğunu söyleyen bir amaç üzerine ilerlediğini beyan etmektedir. 2011 yılında Türk hükümeti tarafından sosyal medya alanında yapılacak olan yasal düzenlemeye karşı bahsi geçen hacker grubu video paylaşım sitelerinden biri olan Youtube'a bir video yayınlayarak 9 Haziran 2011 de Telekomünikayson İletişim Başkanlığının web sitesine saldırı yapacağını duyurmuştur. 2010 yılında başlamış olan arap baharı olaylarını ülkemize taşıma gayreti içerisinde olduğu tahmin edillen grubun bir kısım üyeleri tarafından sergilenen bu çıkışa karşı gönüllü Türk Hacker timleri tarafından saldırı henüz yapılmadan grubun web sitesi çökertilerek cevap verilmiştir. Grup Şubat 2012 yılında da Ermeni Soykırımını devletin tanımasını istemiş hatta bu talebe Redhack (Kızıl Siber Korsanlar) grubuda destek vermiştir. Adelet ve Dışişleri Bakanlığı ile Emniyet Müdürlüğü sitelerine yaklaşık 2 saat boyunca süren saldırılara TİB'de görev yapan uzman ekiplerimiz tarafından karşılık verilerek saldırılar etkisiz kılınmaya çalışılmıştır. 2015 yılında ise Türkiye'nin DEAŞ (Dawlah al-Islamiyah fil-'Iraq wa ash-Sham) terör örgütüne destek veridğini iddia ederek saldırılar yapmaya çalışan Anonymous grubuna Türk hacker timleri tarafından gereken cevap verilmiş sitelerine erişim dahi yapamayan grup Türkiye saldırı yapmaktan vazgeçip adeta kendilerine saldırmaması için Türk Hacker timlerine yalvarmıştır.



Şekil 3.12. Saldırı sonrasına ilişkin Anonymous açıklaması, Kaynak: Ayyıldız TİM, https://l24.im/Od6m

Buna ilişkin Anonymous'un yapmış olduğu açıklama yukarıdaki görselde (Şekil 3.12) görüldüğü üzere Ayyıldız TİM'in hesabından paylaşılmıştır. (Hasan Çiftçi 2013– Sy. 181)

3.1.21. OpIsrael operasyonu

İsrailin 2012 yılında kendisine saldırıldığını iddia ederek başlatmış olduğu Gazze saldırılarına karşı dünyada geniş hacker kitlelerini bünyesinde barındıran Anonymous ve Redhack grupları İsraile karşı "OpIsrael" adını verdikleri bir siber saldırı başlatmıştır.

Şekil 3.13 Anonysmous saldırı açıklaması, Kaynak: https://l24.im/7c8SuG

Bu saldırı yukarıda görüldüğü üzere (Şekil 3.13) çeşitli internet platformları üzerinden duyurulmuştur. Siber saldırı eylemi sonrası Op_Israel adlı Twitter hesabı üzerinden Anonymous grup sözcüsünün yapmış olduğu açıklamda 100.000'den fazla internet sitesinin,

5.000 Twitter hesabının, 40.000 Facebook hesabının ve 30.000 civarında İsrail banka hesabının eylem sonrası bir kısmının kullanılmaaz hale geldiği bir kısmının ise geçici bir süre ile işlem yapamadığı ifade edilmiştir. Yapılan siber saldırı sonrası oluştuğu tahmin edilen maliyetin İsral'de yaklaşık 3 milyar dolar civarında maddi zarara sebep olduğu belirtilmiştir.[4] Anonymous ve Redhack gruplarından yapılan açıklamalarda çocukların öldürülmesine asla göz yummayacaklarını, siyonist devletin masum insanlara zarar vermesini izleyemeceklerini belirttiği ifadeleri basında geniş yer bulmuştur. [5]

3.1.22 Wikileaks / Assange ve Edward Joseph Snowden olayları

Şekil 3.14. Jullian Paul ASSANGE, Kaynak: https://l24.im/Tl0Gxi

Wikileaks, anonim olan çeşitli yerlerden edinmiş olduğu kaynaklara dayanarak devletlerin ve ünlü isimler hakkkında hassas belgeler yayınlayan ve kâr amacı olmadığını ifade eden uluslararası bir sivil toplum kuruluşu olduğunu beyan eder. 2006 yılı ortalarında yaklaşık 2016 yılına kadar 10 milyon belge yayınlayan Wikileaks "Biz Hükümetleri Açarız!" sloganıyla birçok devletin kabusu olmuştur. Sitenin kurucusu ise Jullian Paul ASSANGE'dır. Tğm dünyaya servis edilen görüntülerde ırak savaşında savaş suçları işleyen ABD askerlerinin resimleri ve videoları tüm dünyada yankı uyandırmıştır. Durumun ciddiyeti servis edilen belgelerle ortaya çıkması üzerine ünlü hacker grubu Anonymous harekete geçerek Bradical Operasyonu adında Amerikan savunma bakanlığına karşı saldırı başlatmıştır. Wikileaks 'in kurucusu olan Jullian Paul ASSANGE hükümetlerin halklarından herhangi bir şeyi saklama hakkının olmadığını savunarak bu süreci organize etmeye devam etmiştir. Sonrasında ise ABD tarafından hakkında kırmızı bültenle yakalama kararı çıkartılan Jullian Paul ASSANGE yurt dışında yaşamaya başlamıştır. Sürekli ülke değiştiren Assange 2006 yılında İngiltere'de bulunan Assange gözaltına alınmış ancak sonrasında belirli bir miktar para karşılığında serbest bırakılrak ev

[4] İsraile yapılan saldırılarda duyurular genelde bu twitter hesabından yapılmıştır. https://twitter.com/Op_Israel -

[5] CNN gibi uluslararası kanallar saldırıya ilişkin detayları paylaştığı videolar hazırlamıştır. Dettaylar için Bkz.https://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html

hapsine alınmıştır. 14 Haziran 2012'de İsveç'e iade edilme riski ile karşı karşıya kalan Assange Ekvator Büyükelçiliği'ne sığınmıştır. 7 yıl Ekvator Büyükelçiliği'nde yaşayan Assange 11 Nisan 2019'da Londra polisi tarafından dışarı çıktığı bir esnada tutuklanmıştır. 20 Nisan 2022 tarihinde ise Assange'ın ABD'ye iade edilmesine karar verilmiştir.

Şekil 3.15. Edward Joseph Snowden, Kaynak: https://l24.im/3P1iX

Benzer bir olayda Amerikalı bilgisayar mühendisi, eski Ulusal Güvenlik Dairesi (NSA) ve eski Merkezi İstihbarat Teşkilatı (CIA) çalışanı olarak görev yapmış olan Edward Joseph Snowden'ın 5 Hazşran 2013 yılında Pentagon da bulunan gizli evrakları sızdırması sonucu yaşanmış Snowden Rusya'ya sığınmıştır. Uzun süre Rusya da sığınmacı olarak kalan Snowden daha sonra oturum hakkı almış son olarak 26 Eylül 2022'de Rusya başkanı Vladimir Putin, Edward Joseph Snowden'e Rus vatandaşlığı veren bir kararnameyi onaylamıştır. (Euronews, 2022) Yaşanan olaylar bir kişinin yapmış olduğu bilgi sızdırma veya bilgi çalma işleminin bazen bir devletin ciddi sırlarını oraya çıkarabileceğini göstermesi bakımından önemlidir. Rusyanın Edward Joseph Snowden'ı ülkesine kabul edip kol kanat olması da aslında düşmanı olan Amerikaya ait bilgilerin elinde bir koz olarak tutulması anlamına gelmektedir.

3.1.23 ABD-Çin-Rusya siber savaşı

Amerika Birleşik Devletleri 21 Ekim 2016 tarihindeki amliyeti en büyük siber saldırılarından birisi ile karşı karşıya kalmıştır. Saldırı Çin ve Rus hackerlar tarafından 14 milyondan fazla IP üzerinden botnet ve zombi bilgisayarlarla gerçekleştirilmiştir. DDoS yani (Distributed Denial of Service) olarak da isimlendirilen bu saldırı türüyle karşı tarafın internete veya ilgili web sitelerine girmesi zorlaştırılmaya mümkünse tümüyle engellenmeye çalışmıştır. 2016 yılında tüm uğraşlara rağmen engellenemeyen saldırı sonrası Ülkenin yüzde 78'inden fazlasının

internetsiz kalmış, tahmini olarak ise maddi zararın 7 milyar doları bulduğu ifade edilmiştir. (Takvim, 2016)

3.1.24 JBS SA'ya siber saldırı

Dünyanın aktif olarak devam eden en büyük taze et üreticisi ünvanına sahip olan JBS-SA Şirketi 2021 yılın içerisinde büyük bir siber saldırıya maruz kalmıştır. Dünyada yaklaşık 20 ülkede 174'den fazla tesisi bulunan şirkete yapılan saldırı bir anda tüm dünyanın gündemine oturmuştur. 2021 yılı Haziran ayında bilgisayar ağları saldırıya uğrayan şirket Kuzey Amerika ve Avustralya'daki tesislerini bir süreliğine kapatmak zorunda kalmış ve üretimini uzunca bir süre durdurmuştur. JBS şirketi ise saldırı yapan gruba 11 milyon fidye ödeyerek sistemlerini yeniden çalışır hale getirebilmiştir. Ancak saldırı bir kezle sınırlı kalmamış olup Romanya ve Ukrayna üzerinden gerçekleştirilen bir kaç saldırı sonrası şirket toplamda 70 milyon dolar fidye ödemiştir. Beyaz Saray'ın sözcülüğünü yapan Karine Jean-Pierre ise yapmış olduğu basın toplantısında ABD'nin konuyla ilgili olduğunu düşündükleri Rusya hükümeti ile temasa geçildiğini ve FBI'ın çalışmalarını yürüttüğünü aktarmıştır. Sonrasında ise bazı saldırganlar tespit edilerek elde ettikleri fidyelere el konulmuştur. Yaşanan saldırının sadece bir fidye talebiyle ilgili olmadığı aslında uluslararası pazara sahip olan devasa şirketlere ve onların sırtlarını dayadıkları ülkelere mesaj verme amacı taşıdığı anlaşılmaktadır. Milyonlarca dolar fidye ödemenin yanı sıra çalışılmayan aksayan süreçte zarar ise milyarca doları bulmuştur. Saldırganların küçük meblağlı bir fidye talep etmeleri de aslında yapılan saldırının başka amaçlar taşıdığını gözler önüne sermektedir. ("JBS SA Saldırı ", 2021)[6]

[6]Olaya ilişkin saldırının detayları ile ilgili video linki: https://www.facebook.com/cnnturk/videos/d%C3%BCnyan%C4%B1n-en-b%C3%BCy%C3%BCk-et /

3.1.25. ABD Colonial Pipeline petrol boru hattı saldırısı

Şekil 3.16. Şirketin dışından çekilen bir görsel, Kaynak: https://l24.im/VnCA2R

ABD'nin Doğu kısmında bulunan eyaletlerin petrol ihtiyacının yaklaşık yüzde 45'ini karşılamakta olan Colonial Pipeline, 07/05/2021 tarihinde bilgisayar korsanlarının siber saldırısa uğramıştır. Günlük günde 2,5 milyon akaryakıt taşınan boru hattına yapılan saldırının Rusya menşeili bir korsan grup tarafından yapıldığı ABD Federal Soruşturma Bürosu tarafından ifade edilmiştir. Bu saldırı 50 milyon tüketiciye hizmet veren şirkete yapılmış olup saldırı sonrası ABD Siber Güvenlik Komutanlığı harekete geçmiş ve saldırının geldiği tahmin edilen serverlara karşı saldırılar yapmıştır. 6 gün boyunca çalışmayan boru hattının ABD ekonomisine zararı 2 milyar dolara yakın olduğu tahmin edilmektedir. (Top, 2021)

3.1.26. İran Natanz nükleer santraline saldırı

İran ile İsrail arasında süre gelen gerginlik ve savaş çığırtkanlıklarına İran'nın Nükleer Santiralinde yaşanan ciddi bir sıkıntı ile bir yenisi daha eklenmiştir.

Şekil 3.17. Saldırıya uğrayan nükleer santral, Kaynak: https://l24.im/l4y5t1

İran'nın İsfahan eyalatindeki Natanz şehrinde bulunan ve Nükleer Faaliyet gösteren santrelde (Şekil 3.17) 11 Mayıs 2021 tarihinde elektrik dağıtım sisteminde aksama yaşanmasından sonra İranlı yetkililer tarafından nükleer santrale karşı bir siber saldırı olduğu basına açıklanmıştır. Saldırının İran Cumhurbaşkanı Hasan Ruhani'nin talimatı sonrası önceki santrifüjlere kıyasla 10 kat daha fazla uranyum üretebilme kapasitesine sahip 164 adet IR6 santrifüj zinciri devreye sokulmasından hemen sonra gerçekleşmesi akıllarda soru işareti bırakmıştır. Yine aynı tesiste 2020 yılı Temmuz ayında yangın çıkmış ve İranlı nükleer bilimci Muhsin Fahrizade'nin ölmüştür. Olaydan bir gün sonra İranlı yetkililer olayın İsrail tarafından gerçekleştirilmiş bir sabotaj olduğu iddia etmiştir. Ancak İsrail saldırıyı resmi bir açıklama ile üstlenmemiş İsrail Kamu Yayın Kuruluşu tarafından İran'ın İsfahan eyaletindeki Natanz Nükleer Tesisi'nde oluşan durumun arkasında Mossad'ın olduğunu iddia ifade etmekle yetinmiştir. İran Dışişleri Bakanlığı Sözcüsü Said Hatibzade ise yaptığı basın açıklamasında saldırıların kendilerini durdurmayacağını bilakis daha fazla uranyum zengileştirmesi yapacaklarını ifade etmiştir. (Güler, 2021)

3.1.27. Arnavutluk/ İran gerginliği

Arnavutluk Başbakanı Edi Rama, 2022 yılı temmuz ayında yapmış olduğu basın açıklamasında İran tarafından ülkesine yönelik "büyük bir siber saldırı" düzenlendiğini ifade etmiştir. Rama, bununla da yetinmeyerek Arnavutluk'un İran ile tüm diplomatik ilişkilerini askıya aldığını bildirmiştir. Rama İranlı diplomatlara ve elçilikte çalışan tüm personele ülkeyi terk edebilmeleri için 24 saat süre vermiştir. Yaşanan saldırı sonra kamu hizmetleri aksamış, devlete ait elektronik alt yapı verilerinin çalındığı ifade edilmiştir. Yapılan siber saldırının İran

tarafından yapılmış olduğu iddiasını güçlendiren en önemli bir sebep ise Arnavutluk yönetiminin İran İslam Cumhuriyetine muhalif olan Halkın Mücahitleri Örgütü'nden binlercesini kendi ülkesine barındırmasına İran'ın bu saldırı ile misilleme yaptığı düşüncesidir. Bu grubun ABD'li Cumhuriyetçilerden destek aldığını iddia eden İran, örgüt üyelerinin kendilerine teslim edilmesi yönünde defaten açıklamalar yapmış ancak batı bu talebe sessiz kalmıştır. Açıklamalardan sonra Ulusal Güvenlik Konseyi'nden de sert bir açıklama yapılarak NATO müttefiki olan Arnavutluk'a her türlü desteğin sağlanacağı ifade edilmiştir. NATO her ne kadar her türlü desteği sağlayacağını ifade etse de konsey ülkelerinden birine yapılan saldırı sonrası 5. maddenin işletilmesine ilişkin herhangi bir irade gösterememiştir. Yaşanan bu olayın önemli yanı ise ilk kez bir siber saldırıya uğramış olan ülke saldırı yapan devletle ilişkilerini kesmiştir. Çünkü 2022 yılına kadar onlarca siber savaş ve saldırı olmuş ancak ABD dahil hiçbir ülke siber saldırıya uğramasının ardından saldırının faili olduğu tespit edilen ülkelerle ilişkilerini kesmemiştir. (BBC News, 7 Eylül 2022)

3.1.28. Rusya/Ukrayna savaşı

14 Ocak 2022 tarihinde Ukrayna'nın resmi kurumlarını ve ülkede bulunan bir kısım elçiliklerin sitelerinin etkilendiği olayda dış işçileri ve eğitim bakanlığı gibi kurumların siteleri çökmüştür. NATO'ya girme konusunda kendi ülkesinde yaşayan bir kısım ayrılıkçı gruplar sebebiyle siyasi karışıklık içerisinde bulunan Ukrayna'nın NATO'ya girmesine başından beri karşı olan Rusya yapmış olduğu bu gibi saldırılarla göz dağı vermiştir. Yaşanan saldırı sonrası Avrupa Birliği'nin dış politikalardan sorumlu sözcüsü Josep Borrell, Ukrayna'nın bu gibi saldırılara karşı kendini savunması için tüm kaynaklarını seferber edeceklerini açıklamıştır. Taraflar arasındaki gerginlik yaşanan bu saldırı sonrası hat safaya ulaşmış Ukrayna alt yapı ve tüm güvenliğinden endişe duyduğunu ifade ederek NATO'ya katılma talebinde bulunmuştur. Bunun üzerine zaten bir Kırım gibi bir kısım Ukrayna toprağını işgal eden Rusya'ya fırsat doğmuştur. Ukrayna'nın NATO'ya girme çabasını savaş sebebi sayan Rusya 24 Şubat 2022 tarihinde Ukrayna'yı karadan işgale başlamıştır. Rusyanın işgal harekatı devam ederken 29 Mart 2022 tarihinde Ukrayna için ulusal çapta hizmet veren en büyük telekomunikasyon şirketi Ukrtelecom büyük bir saldırıya maruz kalmıştır. Yaşanan saldırı sonrası internete bağlanma oranları %13 seviyelerine düşmüştür. Günümüz dünyasında yaşanan olayların anlık olarak internet alt yapısı üzerinden paylaşıldığı bir ortamda internetin olmayışı ve telekomünikasyon sisteminin çökmüş olması konvansiyonel silahlarla yapılan müdahaleden daha etkili olmaktadır. Bu durum Ukrayna savaşında da bariz olarak görülmüştür. Yaşanan kesinti üzerine Ukrayna başbakan yardımcısı Mykhailo Fedorov tarafından sosyal medya üzerinden SpaceX şirket Ceo'su Elon Musk'a Starlink uydularını aktifleştirerek kendilerine uydu üzerinden internet sağlaması talebinde bulunmuştur. Anonymous gibi gruplarda yaşanan savaş sırasında Ukrayna tarafında yer alarak Rusya'nın Belarus üzerinden saldırı yapmak için asker taşıdığı tren istasyonu sistemlerine

saldırılar düzenlemiş bu sebeple askeri sevkiyatlarda aksamalar olmuştur. (Çelik, 2022) [7] Yapılan siber saldırılar sonrası bir açıklamada Beyaz Saray Ulusal Güvenlik Konseyi sorumlu danışman yardımcısı Anne Neuberger'den gelmiştir. Neuberger Ukrayna'ya Teknik destek verecelerini ve birlikte bu siber savaşa ilişkin mücadeleyi yürüteceklerini açıklamıştır. Bununla birlikte STM ThinkTech tarafından yayınlanmış olan raporlara göre Rusya 24 Şubat'ta Ukrayna'ya karşı başlatmış olduğu işgalin ilk günlerinden Nisan 2022'ye kadar Ukrayna'nın askeri ve devlet kurumlarına yönelik çevrimiçi saldırılarını yüzde 196 artırdığı tespit edilmiştir. (STM ThinkTech, 2022) Bu da konvensiyonel saldırılarla birlikte siber saldırıların ne kadar ciddi bir öneme sahip olduğunu bir kez daha göstermiştir.

3.2. Siber Savaşın Ekonomik Etkisi

Siber savaşlar genellikle bir bilgisayar ve birkaç yazılım aracılığı ile yapılabilen ucuz maliyetli saldırılar olmakla birlikte vermiş oldukları hasar ciddi boyutlara ulaşmaktadır.

Örneğin yukarıda belirtildiği üzere 14 Ağustos 2003 tarihinde gece saatlerinde gerçekleşmiş olan ve yaklaşık 50 milyon insanın etkilendiği ABD ve Kanada ülkelerin şehirlerini vuran kesinti sonrası saldırının ABD'ye maliyetinin 10 milyar doları bulduğu ifade edilmiştir. Aynı şekilde Kanada da Ontario'da ise üretimin aksamasından sonucu zarar yaklaşık 2,3 milyar Kanada dolarıdır. Yapılan saldırı sonrası ABD'nin dünyadaki en büyük ekonomiye sahip olan ülke olduğu düşünüldüğünde 4 gün boyunca çok büyük eyaletlere elektrik verilememesinin ABD'nin dış ticaretindeki kaybının ne kadar büyük olduğunu anlamamızda kolaylık sağlayacağı açıktır. Yapılan olan ihracatları etkilemesinin yanı sıra buna benzer elektrik kesintilerinin olmaması için alınacak olan önlemler özellikle devletler açısından ekstra maliyete yol açacaktır. Yine saldırı sonrası elektriğin verilememesi sebebiyle sadece devlet kurumları değil o eyaletlerde yaşayan yüzbinlerce insan ve buna bağlı binlerce şirkette bu saldırı sonra ciddi ekonomik kayıp yaşamıştır. Saldırıcı sonrası yaşanan gelişmelere kısaca bakacak olursak bölgede bulunan onlarca petrol rafinerisi ve fabrika 4 gün boyunca çalışamamıştır. Kesinti sonrası şehirlerin ulaşımında kullanılan metrolar ve tren seferleri durmuş, trafik ışıklarının çalışmaması sebebiyle binlerce kaza olmuş, soğuk hava depolarının yetersiz kalması sebebiyle milyonlarca ton gıda bozulmuş, jeneratörlerin çok kısıtlı olması sebebiyle sağlık kuruluşlarında bulunan yoğun bakım üniteleri dahi çalışamaz duruma gelmiş, birçok alanda çok ciddi aksaklıklar oluşmuştur. Yani yapılan bir saldırının yan kollardaki etkileri de bazen saldırının merkezde bıraktığı etti kadar veya beklenilenden daha da büyük olmaktadır.

Yine 2016 yılında ABD-ÇİN-RUSYA siber savaşında Amerikan hükümetine ait kurum ve kuruluşlarına ait birçok site çökertilmiştir. Bu saldırılar DDoS yani zombi bilgisayarın birlikte saldırıları şeklinde olmuş olup ABD'nin %78'inden fazlası internetsiz kalmış ve ülkenin

[7] Tekomünikasyon şirketine saldırının detayları için bakınız. https://www.bbc.com/turkce/haberler-dunya60911853

ekonomisine tahmini zararı 7 milyar dolar maliyetindedir. Bu saldırılar Çin malı akıllı cihazlar üzerinden yapıldığı tahmin edildiği için ABD bir süre Çin malı alımını durdurmuş olup ekstra ekonomik kayba uğramıştır. (Takvim, 2016, 22 Ekim),

Yakın tarihimizde 7 Mayıs 2021 de ABD'nin en büyük boru hattı olan Houston'dan New York Limanı'na petrol taşıyan Colonial Pipeline'a yapılan saldırının Rusya tarafından yapıldığı ABD Federal Soruşturma Bürosu tarafından ifade edilmiştir. Bu saldırı 50 milyon tüketiciye hizmet veren şirkete yapılmış olsa da saldırı sonrası ABD Siber Güvenlik Komutanlığı harekete geçmiş ve karşı saldırılar yapmıştır. 5 gün boyunca çalışmayan boru hattının ABD ekonomisine zararı 2 milyar dolara yakın olduğu tahmin edilmektedir

Siber Saldırıların ekonomik anlamda vermis oldukları hasarların değerlendirilmesi yapılırken elbette ülkelerin kritik alt yapılan yapılan müdahalelerin ne denli etkili olduğu yukarı da verilmiş olan örneklerden anlaşılmaktadır. Bu kapsamda ülkelerin kritik dzüeydeki alt yapılarının korunması büyük önem arzetmektedir. Şöyle ki örneğin su sisteminde yaşanacak bir aksama, su arıtma sisteminde bazı sistemlerin çalışmaması veya arıtma sistemindeki bazı etmenlerin devre dışı bırakılması milyonlarca insanın yaşamış olduğu bir şehirde ciddi sağlık sorunlarına yol açabilecek ve akabinde sağlık sisteminin bel kemiği olan hastaneler kapisete aşımı sonrası işlevsiz hale gelebilecektir. Yine bir diğer kritik alt yapı olan sağlık sisteminde yaşanacak bir sıkıntı tüm ülke genelinde kaos oluşturabilecektir. 2020 yılında baş gösteren ve labaratuvar ortamında oluştuğu tüm dünyaca kabul edilen corona virüs salgını da aslında tam da sağlık sistemi kötü olan ülkelere yapılmış en büyük saldırılardan biri olarak karşımıza çıkmaktadır. Çin üzerinden tüm dünyaya yayılan virüs milyonlarca insanı öldürmüş ve milyonlarcasında da ağır tahribat bırakmıştır. bBir diğer alt yapı sistemi olan bilgi ve telekomünikayson sisteminin hasar alması son yaşanan Ukrayna – Rusya savaşında da görüleceği üzere insanların birbirleri ile olan iletişimi kesmekte ve tüm dünyadan izole etmektedir. Bilişim sisteminin bu derece hasar görmesi bazen ülkeye atılacak yüksek derecede hasas füzelerden hatta kitle imha silahlarından daha etkili olmaktadır. Bu durum gerek yukarıda bahsedilen körfez savaşında gerekse Ukrayna'ya karşı Rusya tarafından başlatılan saldırılarda daha iyi görülmekte ve anlaşılmaktadır. Bir diğer altyapı olan bankacılık ve finans sektörünü hedef alan bir siber saldırı sonrası ekonomik krizin yaşanacağı insanların panikleyeceği muhakkaktır. Banka sistemlerinin çalışmaması sonrası insanların paralarına ulaşamayacağı endişesi bile toplumda bir kaos oluşşturmak için yeterli olabilmektedir. Tüm bunların yanında ulaşım, enerji ve gıda sektörü gibi ülkelerin alt yapılarına yapılan saldırılar yukarıda verilen örneklerde görüldüğü üzere ciddi ekonomik kayıplara neden olmaktadır.

Siber saldırıların ve ülkelerin bu saldırılara karşı yapmış olduğu savunmanın ekonomik boyutu yukarıda örneklerde ortaya koyulduğu üzere ciddi boyutlara ulaşmaktadır. Bu kapsamda Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporları ve Dünya Ekonomik Forumu (WEF)'nun her yıl hazırladığı " 2020 Global Risks Report " raporları incelendiğinde 2011 yılında 1 trilyon dolar, 2015 yılında 3 trilyon doları bulan siber saldırı ve

siber savaş maliyetinin 2021 yılında 6 trilyon dolara ulaşması tahmin edilmiştir. (WEF_Global_Risk_Report , 2020) Yani Amerika ve Çin ekonomisinden sonra siber saldırıların ülke olarak düşünülmesi halinde dünyada 3. Büyük ekonomi olduğu varsayılabilir. Yapılan yeni araştırma verilerine göre ise 2025 yılında yıllık siber saldırı maliyetlerinin 10,5 trilyon dolara ulaşması tahmin edilmektedir (Morgan, 2020)

3.3. Siber Savaşın Siyasete Etkisi

Bilgi alanında iletişim teknolojilerinin gelişmesiyle haberleşme ve sosyal yaşamda da değişimler yaşanmış yaşanmaya da devam etmektedir. İnsanlar çeşitli sosyal medya ağlarından ve değişik haberleşme kanallarından siyasi düşüncelerini her herhangi bir alana bağlı kalmadan ifade edebilmektedir. Ancak iletişimin bu kadar gelişmiş olması her zaman olumlu sonuçlar doğurmamış bazen siyasilerin siyasi hayatlarına bazen de doğrudan kendi hayatlarını kaybetmelerine mal olmuştur. Devletler kendi stratejileri çerçevesinde başka ülkelerin siyasetlerine ve toplumsal yaşamlarına zaman zaman müdahalelerde bulunup manipülasyon yapmış ve algılar oluşturarak iç siyaseti kendi çıkarları doğrultusunda dizayn etmeye çalışmıştır.

Siber alan içerisinde suça yöneltici toplumsal düzeni tehdit eden oluşumlar halklar üzerinde kin ve nefreti körüklemekte olup buna ilişkin eylemlerin engellenmesi toplum güvenliği açısından elzem hale gelemektedir. Toplumsal huzuru bozacak olan eylemler günlük hayatta karşılabilceğimiz sorunlar olabileceği gibi siber ortamda da karşımıza çıkabilmektedir. Örneğin yaşanan bir siber güvenlik saldırı sonrası ülkedeki elektrik sisteminde yaşanabilecek bir sıkıntı doğal olarak toplumun yapı taşı olan bireylere yansıyacaktır. Bunun akabinde siyasi otoriteye olan güvenin sarsılması yapılan saldırının siyasi boyutununda yatsınamayacak derecede önemli olduğunu göstermektedir.

Siber savaşların siyasete etkisi anlamak için en önemli örneklerden biri 2010 yılında Tunus'ta başlayan ve birçok Afrika ülkesine yayılan Arap Baharı adıyla anılan iç ve dış destekli karışıklıklardır. Halk hareketlenmesi olarak da görülen isyan hareketleri çeşitli ülkeler tarafından gerek sözlü gerekse de siber saldırılar ile desteklenerek birçok ülkede on binlerce insanın ölümü ve siyasal rejim değişikliklerine sebep olmuştur. Bu isyanlara doğrudan destek veren Anonymous grubu, Tunus'ta meydana gelen ayaklanma esnasında Tunus'lu hackerlarla ile beraber devlete ait sekiz internet sitesini çökertmiştir. Bu şekilde ülke içerisinde olayların başlamasından hemen önce sonra devlet kurumlarının çalışmasına engel olan siber gruplar göstericilerin isyan hareketlerini hem körüklemiş hem de destek olarak sonuca ulaşmasında etkili olmuştur.

Siber savaşlarda sadece karşı tarafa sosyo-ekonomik zararlar vermek düşüncesi ile değil aynı zamanda yukarıda ifade ettiğimiz gibi bir egemen devlete veya yönetime siyasi olarak baskısı şeklinde de olabilmektedir. 2010 yılında gerçekleştirilen Myanmar hükümetine karşı siber

saldırılar bu duruma güzel bir örnek olarak gösterilebilir. Myanmar seçimleri öncesinde internet ağı DDos saldırılarının hedefi olmuştur (BBC News, 2010, 4 Kasım) Bu saldırılarla Arap baharında olduğu gibi seçim öncesi ve esnasında bilgi akışı siber saldırılar ile engellenmeye çalışılmıştır.

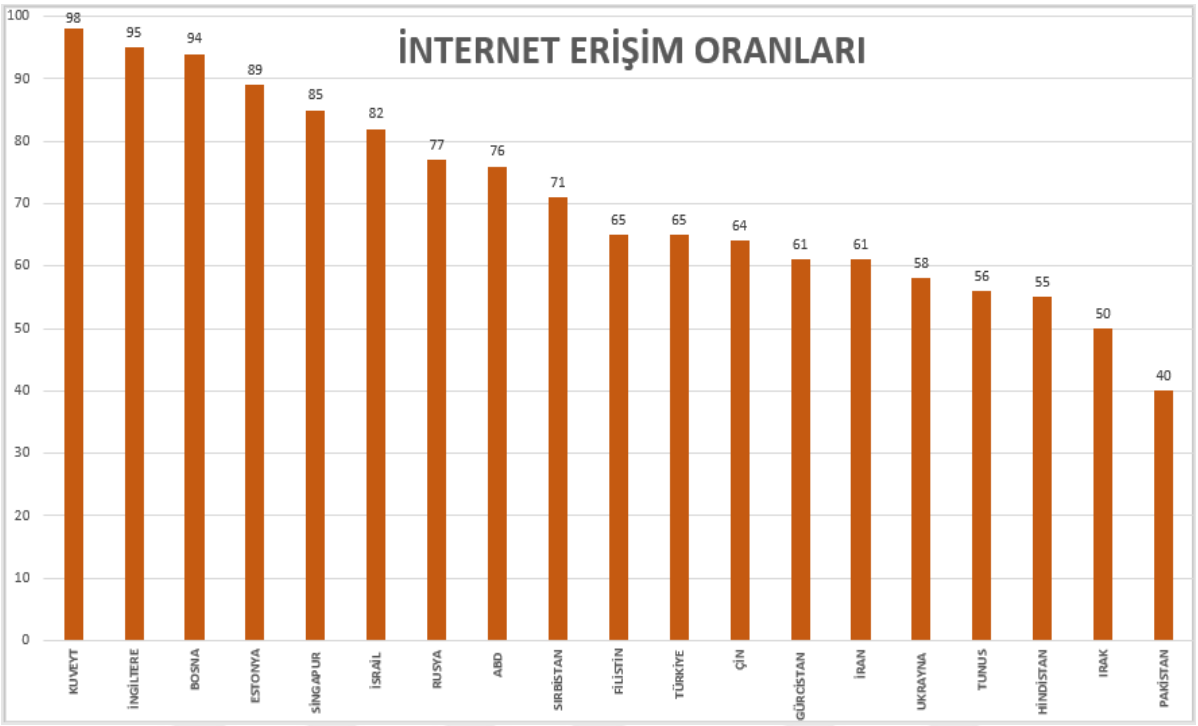
Yine yakın zamanda saldırılarına şahit olduğumuz İsrail-Filistin mücadelesinde 2013 yılında yüzlerce sivil insanın ölümüne neden olan İsrail'e karşı Anonymous gurubu tarafından bir saldırı başlatılmıştır. Yukarida detayları verilen "OpIsrael" adlı saldırılara birçok uluslararası siber örgüt de destek vermiştir. Redhack ve Anonymous guruplarının açıklamasına göre İsrail devletine ve İsrail Savunma Gücüne ait uzantılara sahip 100 bini aşkın internet sitesi, 40 binden fazla Facebook hesabı ve 30 bin civarında banka hesabı bu saldırılardan etkilenmiştir. Bunun üzerine sadece siber saldırılar üzerinden yaklaşık 3 milyar dolar zarar eden İsrail hükümeti saldırılarına son vermiştir.

Yukarıda verilen örneklerden özetle yapılan bir saldırıyla hedeflenen amaçlardan birisi de ülkede korku ve panik yaratmaktır. Yapılacak olan bir siber saldırı ile bilişim sistemleri kullanılarak ülkelerin enerji sistemine verilecek olan hasar ülkede kaosu tetikleyebilecektir. Yine bir baraj kapağının siber saldırı ile açılmış olması belki de binlerce insanın yaşadığı bölgelerde ani sel baskınlarına sebep olabilecektir. Ülkedeki hava kontrol sisteminin ele geçirilmesi sonrası uçak kazaları olabileceği gibi, devasa fabrikalardaki karışım gıda karışım oranları değiştirilerek binlerce insanın hastalanmasına hatta ölümüne sebep olunabilcektir. Bu kapsamda tüm bu örnekler ve varsayımlar değerlendirildiğinde yaşanabilecek olan bu gibi sıkıntılar ülkede kaos oluşturacak ve hükümetlerin istifasına hatta Arap baharı örneğinde olduğu gibi ülkelerin parçalanmasına sebep olmaktadir. (Bayraktar 2015, sy 142)

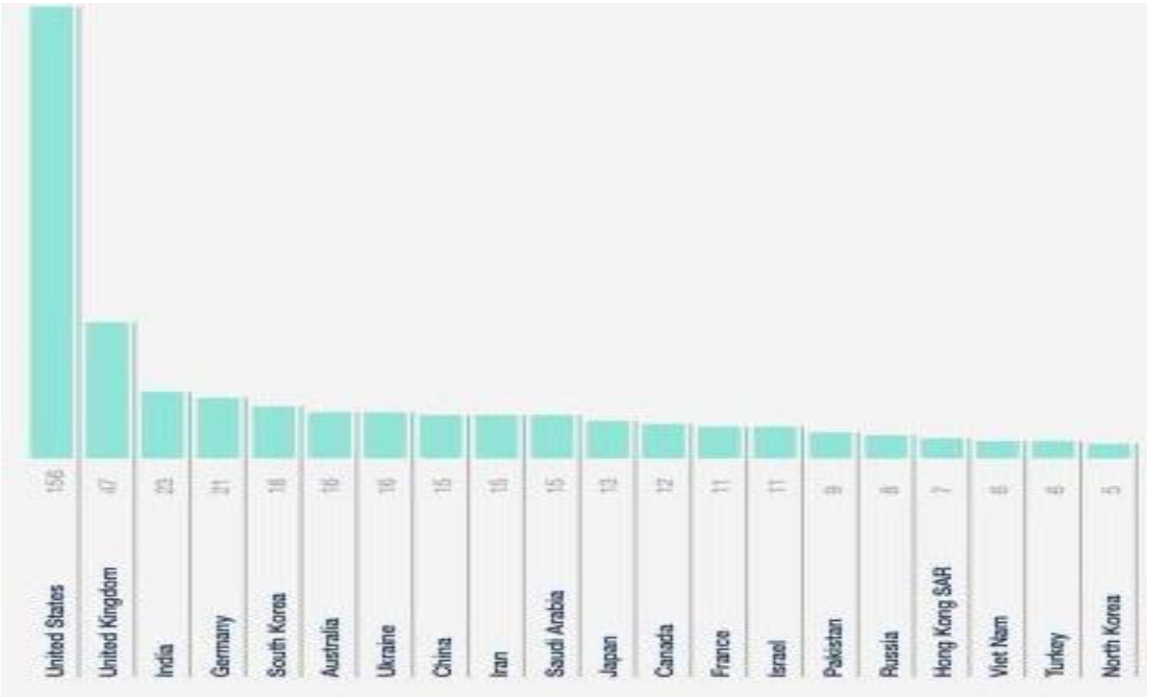
3.4. Siber Savaşın Toplum ve Medya Boyutu

Siber savaşlar ülkelerin ekonomilerini, siyasi geleceklerini etkilediği gibi toplumların yaşamlarında da büyük değişime ve etkiye neden olmaktadır. İnternet kullanımının yıllara göre tüm dünyada artması sosyal medyanın giderek yaygınlaşmasına neden olmuştur. Toplumun ana unsuru olan şahıslara ait kişisel veriler, banka kartı bilgileri, mail adresleri, sosyal paylaşım hesaplarındaki üyelik bilgileri, sağlık, eğitim, iletişim, damar ve parmak izi gibi şahsa ait verin sosyal ortamlarda siber saldırılar ile paylaşılması toplumsal sorunları da beraberinde getirmiştir. İnsanların bilgilerin çalınacağı korkusu ile yaşaması güven kaybına yol açmıştır. İnsanların çeşitli amaçlar kullandığı uçak, tren, metro hatları gibi ulaşım hizmetleri, finans-bankacılık hizmetleri, içme suyu, doğalgaz, elektrik dağıtım merkezleri, sağlık hizmetleri gibi hayatımızın devamı için gerekli olan bu hizmetler bilgi ve iletişim teknolojilerine bağlı olarak çalışmaktadır. Tüm bunlara yapılacak olan herhangi bir siber saldırının ciddi sorunlara yol açacağı açıktır. Bu durumun bir siber savaş boyutunda olması bazen toplumsal felaketlere bile neden olmaktadır.

Tablo 3.2. - 2021 We Are Social Raporu Verileri ve Wikipedia 2020 verileri dikkate alınarak ülkelerin nüfuslarına göre internete erişim oranları verilmiştir



Tablo 3.3. Stratejik ve Uluslararası Çalışmalar Merkezi'nin (CSIS) 2003-2020 yılları arasındaki siber saldırıya uğrayan ilk 20 ülkenin verileridir [8]



2021 We Are Social Raporu üzerinden hazırlamış olduğumuz istatistik verilerinde görüleceği üzere internet kullanım oranları yüksek olan ülkeler de siber saldırıların ve siber savaşların yoğunlukta olduğu tespit edilmiştir. Aynı şekilde sosyal medya kullanımı da siber savaşın genişlemesine olanak tanımıştır. Sosyal medya üzerinden insanların ve kurumların bilgileri çalınabilmektedir. Bununla birlikte Arap Baharı örneğinde olduğu gibi siyaseti dizayn etmek için de sosyal medya etkin rol oynamaktadır. Bu durum siber savaşçıların işlerini kolaylaştırmaktadır. Sosyal medya üzerinden bilgi kirliliği ve karalama kampanyaları ile ülkelerin itibarları yer bir edilmektedir. Ekonomiler de sosyal medya üzerinden yapılan spekülasyonlar ile zaman zaman ciddi zararlara uğramaktadır. Sosyal medya siber savaşçılar için bulunmaz bir bilgi hazinesidir. Siber saldırganlar ve arkasındaki destekleyen uluslararası güçler bu ağı kullanarak ülkelerin iç ve dış siyasetlerine ciddi zararlar oluşturmaktadır.

[8] Bkz. https://www.globalsecuritymag.fr/Germany-and-France-among-the,20200713,100602.html

4.BÖLÜM
ÜLKELERİN GÜVENLİK STRATEJİLERİ

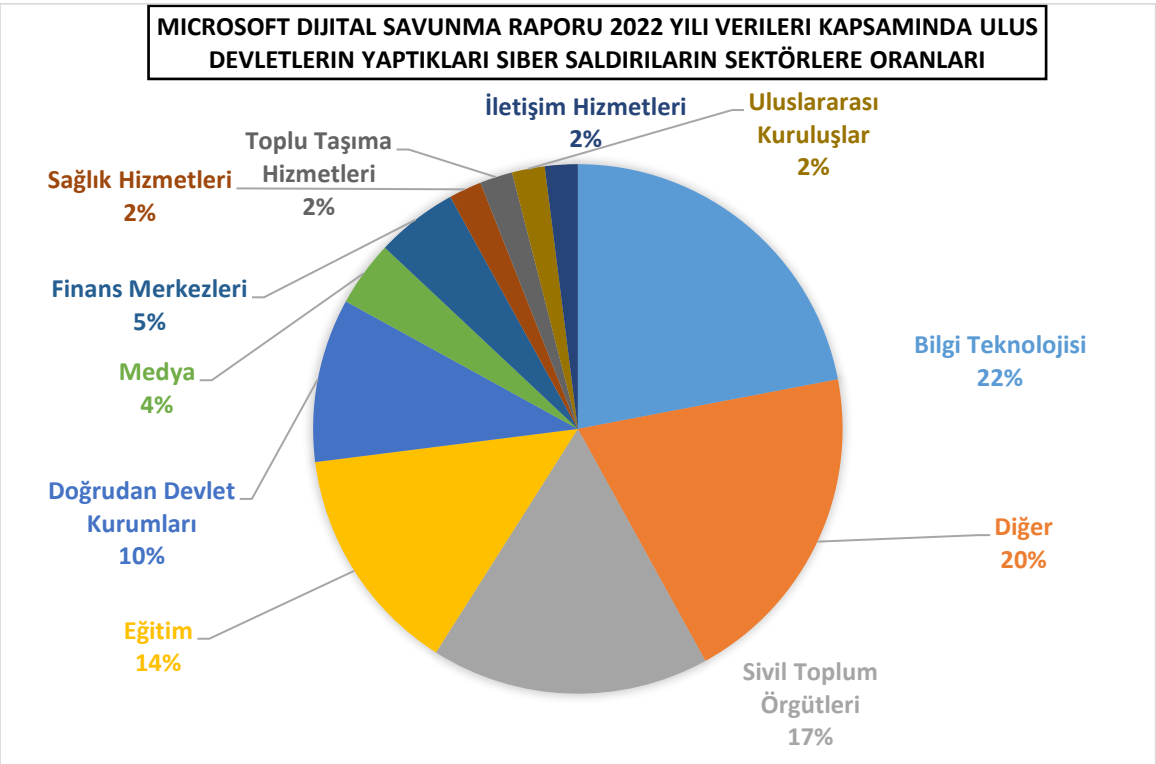
4.1. Siber Güvenlik

Türkiye'nin 2020-2023 Ulusal Siber Güvenlik Eylem Planında, siber güvenlik kavramı "Siber uzayı oluşturan bilişim sistemlerinin tehlikeli siber ataklardan korunmasını, bu alanda işlenen verinin/bilginin gizliliği, bütünlüğünün ve erişilebilirliğinin koruma altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı önlem mekanizmalarının devreye alınmasını, sistemlerin yaşanan saldırı öncesi durumlarına geri döndürülmesini sağlayan faaliyetler bütünü" olarak tanımlanmıştır. (Ulaştırma Bakanlığı Eylem Planı, 2020, s.10)

Genel olarak siber güvenlik denildiğinde kurumların ve kullanıcıların benliklerinin korunması düşüncesiyle çeşitli eğitimlerin, faaliyetlerin, uygulama ve teknolojilerin bir bütünü oluşturması akla gelmektedir. Siber güvenliğin 3 temel prensibi olan erişilebilirliğin, bütünlüğün ve gizliliğin korunması için gerekli alt yapıların oluşturulması ve savunma stratejilerinin geliştirmesi her ülke için elzemdir. Yaşanan çağ siber saldırılara ve savaşlara karşı yeni güvenlik politikaları geliştirmeyi zorunlu kılmaktadır. Bu kapsamda ülkelerde siber güvenlikleri açısından çeşitli güvenlik yazılımları ve uygulamalar geliştirerek güvenlik duvarları oluşturmakta, siber saldırı eylem planları hazırlayarak siber savaşlara karşı bireyleri bilinçlendirmeye çalışmaktadır. Yapılan araştırmalar sonucu aşağıda da belirtileceği üzere ülkelerin bilişim sistemlerini sürekli güncellemeye çalıştıkları, bu sistemlerde oluşabilecek açıkların tespitini için kısa periyotlarla zafiyet taramaları yaparak raporlar oluşturduğu anlaşılmıştır. Ülkeler siber güvenliklerine ilişkin olarak bazen kendileri tarafından geliştirilmiş bazen de bir güvenlik şirketinden alınmış tarama ve antivirüs programlarını kullanarak sistem içerisinde bulunan zararlı yazılımları tespite ve sonrasında temizlemeye çalışılar. Örneğin güvenlik duvarı oluşturarak yerel ağlardaki iletişimi kontrol edebilirler. Elektronik imza gibi içerisinde yerleştirilen yazılım sayesinde şifrelenmiş imzaları kullanarak bilgilerin kimden geldiği ve kimin aldığı noktasında güvenli iletim oluştururlar. Ayrıca ülkeler kullanıcıların ağ portlarını, protokolleri ve hizmetleri kontrol ederek veri güvenliğini sağlamaya çalışmaktadır.

Siber Güvenlik denildiğinde dünyanın en büyük çok uluslu teknoloji şirketi Microsoft'un en güncel siber güvenlik raporuna bakılması yerinde olacaktır. Bu rapor kapsamında şirketin kendi sistemlerinde bulunan güvenlik programları üzerinden ulus devletlerden aldığı veriler kapsamında 2019 yılı ile 2022 yılı haziran ayı arasında olan saldırıların hangi sektörlere karşı yapıldığı Tablo 4.1'de istatiksel olarak gösterilmiştir.

Tablo 4.1. Microsoft Şirketi tarafından hazırlanan 2022 yılı siber savunma verilerinden yararlanılarak hazırlanmıştır. Kaynak: https://l24.im/s90AlTS, sy 36



Bu veriler toplanırken Rusya ve İran üzerinden gelen saldırıların yoğunluğu dikkat çekmiştir. Görüldüğü üzere ülkeler bir başka ülkeye saldırı yaptıklarında ülkenin önemli teknolojik sistemlerine karşı saldırıları öncelemiştir. Sonrasında ise ülkelerin bel kemiğini oluşturan sivil toplum örgütleri ve devlet kurumlarının hedef alındığı görülmektedir. Microsoft şirketi alınan verilere göre 2019 yılından bu yana kritik alt yapılara olan saldırıların ortalama %40 oranında arttığını tespit etmiştir. Bu veriler devletlerin güvenlik stratejilerini belirlemelerinde önemli bir etkiye sahip olmalıdır. Zira saldırılar önceki yıllara göre doğrudan devlet kurumları hedef almak yerine çeşitli alt yapıları çökertmeye doğru evrilmiştir. Bu kapsamda eğitim, sağlık, ulaşım gibi alt yapılara yapılan saldırılar son dönemde giderek artmıştır.

4.2. Ülkelerin Siber Alanda Aldıkları Önlemler

Aşağıda örneklem analiz yöntemi kullanarak en fazla siber savaş tecrübesi yaşamış ülkelerden bazılarının bu saldırılara karşı yapmış oldukları savunma stratejilerine örnekler verilecektir.

4.2.1. ABD'nin siber güvenlik politikaları

Devletlerin güvenlik politikalarına bakıldığında yargısal düzenlemeler ve güvenlik stratejilerin ABD tarafından uygulandığı görülmektedir. Bilişim teknolojileriyle bağlantılı suçlara ilişkin olarak 1984 tarihinde ilk federal yasa olan "Bilgisayar Dolandırıcılığı ve Bilgisayarların Kötü Amaçlı Kullanılması Kanunu (Counterfeit Access Device and Computer Fraud and Abuse Act)" kabul etmiştir. 1994 yılına gelindiğinde "Ortak Güvenlik Kurulu" kurulmuş olup ağ teknolojilerinin yayılmasının oluşturduğu riskler ele alınmıştır. 1995 senesinde de Ulusal Savunma Üniversitesi "siber savaşçı" isimli ilk mezunlarını vermiştir. 2008 yılına gelindiğinde ise Beyaz Saray içinde Siber Güvenlik Ofisi kurulmuştur. Bu yaklaşım kapsamında yeni güvenlik stratejileri ortaya konarak federal sivil ağların korunması, istihbarat toplanması karşı atak ve ordu ağı savunması sağlanması üzerinde çalışmıştır. Bunlara ilaveten yukarıda ifade edilen ilk 3 aşama için birlikte kullanılan EINSTEIN, TIC ve Classified Programı gibi bazı bilgisayar programları geliştirilmiştir. (ÜNAL 2012, 14)

21 Mayıs 2010 tarihine gelindiğinde ise Siber Komutanlık - CYBERCOM kurulmuştur. Son olarak Amerika Birleşik Devletleri'nin günümüzdeki siber güvenlik politikasına değinecek olursak 2017 senesinde Devlet Başkanı Donald Trump verdiği ilk bütçe teklifine bakıldığında federal devletler ile Amerika Birleşik Devletleri'nin kritik altyapılarının savunulması amacıyla siber güvenlik çalışmalarına 1.5 milyar dolar yatırım desteği verileceği ifade edilmiştir.(Varlık, 2017)

4.2.2. Çin Halk Cumhuriyeti'nin siber güvenlik politikası

Çin denildiği zaman akla dünyanın en kalabalık ülkesi gelmektedir. Bununla birlikte dünyanın her yerine dijital ürün ihraç eden en büyük ekonomiye sahip ülke olduğu ekonomi verileri ile ortadadır. Bu da Çin hükümetinin öncelikle hem ülkesindeki sosyal medya üzerinden yaşanabilecek siber saldırı problemleri en aza indirmek hem de ekonominin güvenliğini sağlamak amacıyla belli başlı önlemler almaya zorlamıştır. Çin ilk önlemlerini 1990 yıllında almıştır. Altın Kalkan Projesi ismiyle zikredilen Büyük Çin Güvenlik Duvarı (The Great Firewall) sistemiyle internetin ve sosyal medya platformlarının kontrolü için 50.000 internet polis görevlendirmiştir. Örneğin Çin'de Youtube, Twitter, Facebook ve benzeri sosyal medya siteleri yasaktır. Bu tarz sosyal medya sitelerine olan gereksinimi gidermek için Çin kendi sınırları içerisinde kopyasını oluşturarak Youtube yerine Youku, Twitter yerine Fanfou, Facebook yerine Renren gibi siteleri kurmuştur. Bu sitelere hükümet tarafından açıkça fondan para ayrılarak desteklenmektedir. Bu şekilde şirketlerin merkezleri bir başka ülkeye bağlı olan ve yönlendirmeye müsait olan platformların ülke içerisinde siber saldırı aracı olarak kullanılması engellenmeye çalışılmıştır. [9]

[9] Çİn'in altın kalkan prohesinin detatları için https://webrazzi.com/2011/05/06/altin-kalkan-projesi-cin/

Çin Ulusal Ordusu Genelkurmay Başkanlığının 3. Departmanı Çin ordusunun kullandığı internet altyapısının güvenliğini sağlamakla yükümlüdür. Siber saldırılara karşı oluşturulan bu birim ülkeye giriş çıkış yapan sinyal istihbaratından elektronik bilginin toplanmasına, analiz edilmesine ve kullanılmasına kadar tüm evrelerinden sorumludur. Bunun yanı sıra 3 adet araştırma şirketi de ülkenin siber güvenliğinin sistemlerinin geliştirilmesi maksadıyla devamlı olarak AR-GE çalışmalar yapmakta ve Çin'in önde gelen yüksek okulları da bu çalışmalara katılmaktadır. (Gül, 2012)

4.2.3. Rusya Federasyonu siber güvenlik politikaları

Siber güvenlik alanında diğer ülkelerde olduğu gibi çeşitli kanunlar çıkaran Rusya "Kara liste Kanunu" ile adlandırılan kanun kapsamında "izinsiz gösteri çağrısı barındıran", "nefret duygusu oluşturan" ve" kurulan düzene aykırı olan" diğer tüm fiillerin, savcılık tarafından mahkeme kararına gerek duymaksızın engellenebileceği kanunla düzenlenmiştir . Yine popüler sosyal medya platformlarına geriye dönük altı aylık bir veri bulundurması zorunluluğu getirilmiştir. [10] yine tüm İnternet servis dağıtıcılarının (ISS'ler), verileri Rusya'nın fiziki sınırları içerisinde bulunan sürücüler üzerinde toplamları zorunluluğu getirilmiştir.

Rusya Federal Teşkilatı, ülkeye karşı iç ve dış kaynaklı yapılan siber atakları öncesinden saptamak ve bu saldırılara karşı tedbir alabilmek için gerekli istihbarat çalışmalarını yürütmekle yükümlüdür. Rusya'nın da tıpkı Çin gibi vatandaşlarının internet ve sosyal medya kullanımına aktivist hareketleri önlemek adına bir takım sansür ve sınırlamalara gittiği görülmektedir. Bu sınırlamaları yaparken Rusya Çin'den farklı olarak hukuki alt yapılarını da hazırlamaktadır. Rusya zaman zaman da savunma mekanizması olarak saldırı politikasına da yer vermektedir. Yani bir yeri savunmanın yolunun çevresindekilere saldırı yaparak güçsüzleştirme politikası izlemek olduğunu ortaya koymaktadır. Rusya'nın kendi siber güvenliğine ilişkin tutumunu özetleyecek olursak bu iki anahtar kavram ile ifade edebiliriz. Birincisi "ulusal internet" ve ikincisi ise "ülkenin savunmasına karşı siber uzaydan gelecek herhangi bir tehdite karşı katı koruma" olarak nitelendirilebilecektir.

4.2.4. Türkiye'nin siber güvenlik politikaları

Türkiye'de siber güvenlik alanında Bilgisayar Olaylarına Müdahale Ekibi (TRBOME), TÜBİTAK bünyesinde faaliyetlerini yürütmektedir. Ülkemizde de yine diğer ülkeler gibi çeşitli kanunlar ve mevzuatlar ile siber güvenliğin sağlanması için bir dizi adımlar atılmıştır. Bunların sonucunda Telekomünikasyon İletişim Başkanlığı yapısı altında siber güvenliğe ilişkin ortaya

[10] Belgenin orjinaline https://cyber.harvard.edu/publications/2014/runet_regulation adresinden erişilmiştir. (Erişim Tarihi: 12/05/2021)

çıkan olaylarda koordinasyonun sağlanmasını için 2013'te Ulusal Siber Olaylara Müdahale Merkezi (USOM CERT) faaliyete geçirmiştir. [11]

TÜBİTAK BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) ve Bilgi Teknolojileri ve İletişim Kurumu beraberliğinde 2011 senesi ocak ayı içerisinde siber savunma ve saldırı tatbikatları gerçekleştirilmiştir. Yine Ocak 2013'te 2. kez Siber Güvenlik Tatbikatı yapılmış olup UDHB'nın ortaklığında BTK ve TÜBİTAK tarafından desteklenen ve siber ataklara karşı savunma amaçlı gerçekleştirilen tatbikata 61 özel sektör ve kamu kuruluşu iştirak etmiştir. Tatbikat 24 Aralık 2012- 11 Ocak 2013 tarihleri arasında yapılmıştır. Tatbikata katılanların büyük bir kısmını kamu kurumları oluşturmasına rağmen özel sektör ve sivil toplum kuruluşlarından da katılım olmuştur. Katılımcılar arasında kritik altyapıların yönetilmesi ve işlerin yürütülmesinden sorumlu kurum ve kuruluşlar tatbikat kapsamında görevlendirilmiştir.

Türkiye ilerleyen dönemlerde siber güvenlik strateji belgeleri hazırlamıştır. Bunların ilki ve temeli 2013-2014 Ulusal Siber Eylem Planıdır. Bu belgede ulusal güvenliğin sağlanması için çeşitli diğer ülkelerin stratejileri ve planlarının incelendiği belirtilmiş, uluslararası toplumdaki ülkelerin katılmış oldukları örgütlerin iş birliği içerisinde çalışması vurgulanmıştır. Daha sonraki dönemde 2016-2019 Siber Güvenlik Stratejisi belgesi yayımlanmıştır. Bu belgede önceki belgeye atıflar yapılarak siber güvenlik alanında gerçekleştirilmesi hedeflenen faaliyetler belirlenmiştir. Bu faaliyetlerden en ilgini çekeni ise "SİBER YILDIZ" olarak adlandırılan bir yarışma yapılacağı açıklamıştır. Bu yarışma sonucunda belirlenecek yetkin kişilerden siber ordu oluşturacakları USOM tarafından ifade edilmiştir. [12]

Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksi'nin 2019'da raporlanan sonuçlarına bakıldığında Türkiye bir önceki senelere nazaran 23 sıra birden yukarı çıkarak 2018'de dünyada 20. sırada, Avrupa'da 11. sıraya yükselmiştir. 2020 yılı verilerine göre ise dünyada 11. sırada avrupada ise 6. sıraya yükselmiştir.

2020-2023 Ulusal Siber Eylem Planında ise bu zamana kadar ki çalışmaların daha iyi hale getirilmesi için nelerin yapılabileceği değerlendirilmiştir. Bu kapsamda 10 Şubat 2020'de Ulusal Siber Olaylara Müdahale Merkezi Cumhurbaşkanın katılımıyla açılmıştır. Ülkemizin 2023 yılı vizyonu çerçevesinde kritik altyapılarının korunması için çeşitli hedefler konmuştur. Bu eylem planı içerisinde "Uydu-Haberleşme", "Ekonomi", "Ulaştırma", "Su- Enerji" ve "Kritik Kamu Faaliyetleri" alanlarında siber güvenliğin arttırılması için ihtiyaç duyulan teknolojik yazılımların milli olmasına özellikle dikkat edileceği ifade edilmiştir.

Ulaştırma ve Altyapı Bakanı Adil Karaismailoğlu 12 Ekim 2021 yılında 2 gün boyunca sürecek Ulusal Siber Kalkan Tatbikatı başlattıkları açıklayarak 36 farklı kurum ve kuruluşun bu tatbikata katıldığını ifade etmiştir. Karaismailoğlu siber saldırıların dünyaya maliyetinin 2021

[11] Detaylı bilgi için (Bilgi Teknolojileri ve İletişim Kurumu Faaliyet Raporu , 2016)

[12] Bkz. Siber Yıldız yarışmasına ilişkin detaylı bilgi için https://www.siberyildiz.com/

yılı için ortama 6 trilyon dolar olduğunu ifade etmiş bu kapsamda Türkiye olarak çeşitli Teknik yazılım ve donanımsal sistemler üzerinde çalışıldığını ifade etmiştir. Tamamen yerli ve milli imkanlarla geliştirilen KASIRGA, AVCI ve AZAD uygulamaları sayesinde son 4 yıl içerisinde Türkiye'yi hedef alan yüz binlerce saldırının engellendiğini ifade eden Karaismailoğlu USOM bünyesinde kayıtlı 6 bin 99 siber güvenlik uzmanının hali hazırda siber sahamızın korunmasına görev yaptığını ve bu alanda kararlılıkla mücadeleyi sürdüreceklerini beyan etmiştir.

SONUÇ/SONUÇ VE ÖNERİLER

Giriş kısmında da ifade ettiğimiz üzere internetin ve dijitalleşmenin hızla geliştiği dünyamızda güvenlik açıkları da oluşmaya başlamıştır. Bilgi ve iletişim sistemleri gelişerek insanlara büyük kolaylıklar sağlamış olsa da sistemlerin kötü amaçlı olarak kullanılması hem ulusal güvenlik hem de ekonomik açıdan büyük zararlara yol açmıştır.
İnternet ilk dönemdeki gibi sadece insanların bilgi edinme, kurumsal işlemlerini hızlıca yapabilme ve sosyal medyada gününü paylaştığı bir alan olmaktan çıkmıştır. Devletlerin neredeyse tamamı kurumsal işlemlerini internet üzerinden gerçekleştirmektedir. Bu işlemlerin içerisinde kritik öneme sahip alt yapı sistemlerinin koordinasyon ve kontrolleri, enerji, sağlık, eğitim, ulaşım, savunma ve haberleşme alanları da bulunmaktadır.

İnsanların ve devlet kurumlarının siber uzay dediğimiz içerisinde hava, kara, deniz ve uzayında içinde olduğu tüm alanları kapsayan 5. Boyut bir ortama bağımlılığının giderek artması bu alan üzerinden saldırıları ve savunmaları da kaçınılmaz hale getirmiştir.

Siber alan üzerinden yapılan saldırıların maliyetinin düşük ancak saldırının sonucunda verilen zararın ciddi anlamda büyük olabilmesi savaş araçlarına büyük yatırımlar yapan ülkeleri bu alana yönlendirmiştir. Bu alanda yapılan bir saldırının nerden geldiğinin tespitinin de bir hayli zor olması saldırganların işine gelmektedir.

Saldırlar sonucu hem bireylerin hem de devletlerin ekonomik kaybı yukarıda ifade edildiği üzere milyar dolarları bulabilmektedir. Bu sebeple bu alanda alınacak önlemler çok önemli ve gizlilik arz eden devletlerin verilerinin çalınmasını önlemek için hayati önem arz etmektedir.

Çalışmamız kapsamında öncelikle siber saldırıların nasıl gelişim gösterdiği örnekler verilerek anlatılmış daha sonra ise bunların ülkeler arasında ne tür savaşlara sebep olduğu, sonuçları açısından da ekonomik, siyasi, toplumsal ve medya boyutları incelenmiştir. Son olarak ise ülkelerin bu siber saldırı ve savaşlara karşı nasıl savunma stratejileri geliştirdiğine değinilmiştir.

Değerlendirilmeye alınan ülkelerin stratejileri incelendiğinde; siber ataklar kapsamında ülkelerin kendilerine karşı yapılacak olan saldırılara ilişkin tehdidin bilincinde oldukları, siber uzay alanını artık ulusal savunma alanı içinde kabul etmeye başladıkları ve AR-GE çalışmalarına hız verdikleri anlaşılmaktadır. Bu durumu siber saldırılara duyarlı hemen hemen tüm ülkeler güvenlik strateji belgelerinde ifade etmektedir. Ayrıca kendi ülkemizde olduğu gibi çoğu ülkede de siber güvenlik kapsamında yasal düzenlemeler yapılmıştır. Ancak bazı ülkelerdeki kanuni düzenlemelerin kişisel hak ve özgürlüklerin kısıtlanmasına kadar gittiği görülmektedir. Bu açıdan siber güvenliğin sağlanması ile kişisel hak ve özgürlük alanınınki çizginin net çizilemediği ortadır.

Bu gelişmeler çerçevesinde ve siber uzaydaki tehditlerin gelişimine bakıldığında hükümetlerin, kişilerin, kamu kurumu ve özel kuruluşların gerekli önlemleri alması gerekmektedir. Devletler kendi kritik alt yapılarını korumak ve bu alt yapıların güvenliğini sağlamak adına internete bağlanan tüm kritik sistemlerinde milli yazılım sistemleri kullanması çok önemli olduğu sonucu ortaya çıkmaktadır. Ayrıca devletlerin yukarıda görüldüğü üzere kendi politika ve stratejilerini belirlemeleri gerekmektedir. Bu strateji çerçevesinde gerek kamu kurumlarının gerek özel sektörün belirli bir hedefe doğru yapılan strateji doğrultusunda ortak hareket etmesi gerekmektedir. Yaşanacak saldırılara karşı savunma mekanizmaları geliştirilirken bunların yasal alt yapılarının oluşturulması da elzemdir. Kanuni olmayan süreçlerin işletilmesi sonrası daha büyük sosyal ve siyasal sorunların çıkacağı muhakkak olup buna ilişkin yasal çerçevenin gerek yasalar gerekse diğer mevzuatlar çerçevesinde belirlenmesi elzemdir. Yine yapılan çalışmamız sonrası çıkan sonuçlardan biri ve en önemlisi de Teknik olarak bu alanda yazılım ve donanım geliştirmelerine ara vermeden devam edilmesi gerekliliğidir. Güncel olmayan yazılımlar ve donanımların siber saldırılara açık olacağı kuşkusuz olup bu alandaki ulus devletlerin eksikliğini bir an önce gidermesi gerekmektedir. Alınacak olan tüm tedbirler tehditlerin vereceği zararın en aza indirilmesi için önemlidir. Ancak sadece tedbir almak bu saldırıları bertaraf etmekte tek başına pek mümkün olacak gibi gözükmemektedir. Bu kapsamda devletlerin ulusal bazda ve uluslararası alanda birbirleriyle entegre çalışmalar yürütmesi ve siber uzayın savunması kapsamında farkındalığı artırmak için toplumu tüm bu tehditlere karşı bilinçlendirmesi gerekmektedir.

KAYNAKÇA

A Shortlist of Reported SCADA Incidents (2009), (Erişim Tarihi 14/11/2022) https://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/

Anadolu Ajansı, (2021, 2 Haziran), " JBS SA Saldırı" (Erişim Tarihi: 10/06/2022)https://www.trthaber.com/haber/dunya/beyaz-saray-jbs-saya-duzenlenen-siber-saldirinin-arkasinda-ruslar-olabilir-585410.html

Anadolu Ajansı, (2012, 20 Kasım), "İsrail ordusu siber savaşı kaybetti" (Erişim Tarihi: 10/06/2022) http://www.aa.com.tr/tr/tag/102397--israil-ordusu-sibersavasi-kaybetti

Arquilla, J., and Ronfeldt, D. (2001). Networks and Netwars The Future of Terror.

Avcıoğlu, Doç. Dr. Gürcan Şevket, (2017) Emek, Sibernetik ve Toplum, https://dergipark.org.tr/tr/download/article-file/325147,(s.33-34)

Bayraktar, Gökhan (2015), Siber Savaş Ve Ulusal Güvenlik Stratejisi, Yeniyüzyıl Yayınları 1. Baskı, İstanbul.

BBC News, (2010, 4 Kasım) " Tüm ülkenin internetini çökerten saldırı", (Erişim 11/12/2022, https://www.bbc.com/turkce/haberler/2010/11/101104_burma_cyber_attack

BBC News, (2022, 20 Nisan) "İngiltere'de mahkeme Assange'ın ABD'ye iadesine onay Verdi", Erişim 11/12/2022, https://www.bbc.com/turkce/haberler-dunya-61162037

BBC News, (2022, 7 Eylül) " Arnavutluk, 'siber saldırı' ile suçladığı İran'la diplomatik ilişkilerini kesti", Erişim 11/12/2022, https://www.bbc.com/turkce/haberler-dunya-61162037https:// www.bbc.com/turkce/articles/cyjv82810xko

Bendiek, Annegret ve Metzger, Tobias (2015), Deterrence Theory in the Cyber Security, Working Paper RD EU/Europe, Berlin: Research division/EU.

Clarke, Richard A. Ve Knake, Rorbert K. (2011), Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit, (Çev. Murat Erduran), İstanbul Kültür Üniversitesi Yayınevi: İstanbul (Sy. 9- 14).

Crime, and Militancy. USA: RAND Corporation. 240-248.

Çelik, Dr. Emine, (2022, 3 Mart), "Rusya Ukrayna Savaşının Siber Boyutu", Erişim 11/12/2022, https://www.aa.com.tr/tr/analiz/rusya-ukrayna-savasinin-siber-boyutu/2522079

Çiftçi, Hasan (2013) Her Yönüyle Siber Savaş , 1. Baskı , TÜBİTAK Popüler Bilim Kİtapları .

Çölgeçen, Mutlu (2002) Siber Savaş Kıyametin İlk Halkası, 1. baskı, Arşiv Kitapları (Sy.38).

DOD Dictionary of Military and Associated Terms: Siber Alan Tanımı. Sy 60, Erişim Tarihi: 15.05.2021. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Euronews, (2022, 26 Eylül), "Snowden'a Rus Vatandaşlığı", Erişim 10/12/2022 https://tr.euronews.com/2022/09/26/putin-abdli-istihbarat-ajani-edward-snowdena-rus-vatandasligi-verdi

Gül, Ahmed Furkan, (2012), "Çin ve ABD İncelemesi", İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü, Siber Güvenlik Raporu, Mayıs 2012, İstanbul, sy: 18.

Güldoğan, M. V. & Işıklı, Ş. (2022). Siber Savaşta Mütekabiliyet. AJIT-e: Academic Journal of Information Technology, 13 (51), 287-319. DOI: 10.5824/ajite.2022.04.004.x .

Güler, Bilal (2021, 12 Nisan), "İran İntikam Alacağını Duyurdu", Erişim Tarihi: 25/10/2021, https://www.aa.com.tr/tr/dunya/iran-natanz-nukleer-tesisindeki-saldiri-nedeniyle-israili-suclayarak-intikam-alinacagini-duyurdu/2205793.

Günal, Bülent, (2011, 7 Şubat), "Mavi Marmara baskını sonrası İsrail'e kafa göz daldık "Erişim 10/11/2022.

Habertürk, (2022, 25 Şubat) "Rusya-Ukrayna-ABD üçgeninde siber savaşta neler yaşanıyor?" Erişim 26/12/2022, https://www.haberturk.com/rusya-ukrayna-siber-savasta-neler-yasaniyor-3356270-teknoloji

Hackers breach defences of joint strike fighter jet programme, (2009), Erişim 10/10/2022 https://www.theguardian.com/world/2009/apr/21/hackers-us-fighter-jet-strike,

Hainan Island İncident, https://en.wikipedia.org/wiki/Hainan_Island_incident

Holat, Olcay (2021) Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. Abant Kültürel Araştırmalar Dergisi, 6 (11): 115-117.).

https://www.salom.com.tr/arsiv/haber/73515/ortadoguda-medya-savaslari-hamasIsrail

https://bulutistan.com/blog/ddos-nedir/

Keleştemur, Atalay (2015). *Siber İstihbarat*, Level Yayınları Kocaeli Üniversitesi, Kocaeli (sy.222).

Kevin D. Mitnick, William L. Simon, (2013) Sızma Sanatı, (çeviren:Emel Aslan), 1.baskı, Ankara (s.288, s.289).

Köprülü, Dr. Tacettin, 10 Nisan 2020 5. Sayı "Geçmişten Geleceğe Sibernetik" Havelsan Dergisi, (Sy. 16).

Libicki, Martin C. (2009), Cyberdeterrence and Cyberwar, Santa Monica: Rand Corporation.

Morgan, Steve (2020) "Özel Rapor: C-Suite'te Siber Savaş", Siber Suç Dergisi, (Erişim 12/06/2021) https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
SAYGILI, İsmail, (2020) "Siber Savaş ve Siber" , 11. Sayı Arka Kapı Siber Güvenlik Dergisi , (Sy.39)

STM Teknolojik Düşünce Merkezi " Rusya'nın Ukrayna İşgali Kapsamında Siber Savaşın Geleceği", Erişim 10/12/2022 https://thinktech.stm.com.tr/uploads//docs/1653303371_stmblogrusyaninukraynayi isgalikapsamindasibersavas.pdf?

Takvim, (2016, 22 Ekim), "Siber Saldirinin Abdye Maliyeti 7 Milyar Dolar" , Erişim Tarihi: 08/10/2022, https://www.takvim.com.tr/dunya/2016/10/22/siber-saldirinin-abdye-maliyeti-7-milyar-dolar

T.C. Ulaştırma ve Altyapı Bakanlığı Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (Sy.10) https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf

T.C. Ulaştırma ve Altyapı Bakanlığı , "SİBER GÜVENLİK ARTIK BİR MİLLİ GÜVENLİK MESELESİ", Erişim 16/11/2022, https://www.uab.gov.tr/haberler/ulastirma-bakani-karaismailoglu-siber-guvenlik-artik-bir-milli-guvenlik-meselesi.

Thornburgh, Nathan (2005), "The Invasion of the Chinese Cyberspies" https://content.time.com/time/subscriber/article/0,33009,1098961-1,00.html
(Thornburgh tarafından kaleme alınan yazı)

Top, Yağmur, (2021) "Colonial Pipeline saldırısı hakkında bilmeniz gereken 5 şey" Erişim Tarihi: 30/10/2021, https://siberbulten.com/kritik-altyapi-guvenligi/colonial-pipeline-saldirisi-hakkinda-bilmeniz-gereken-5-sey/

U.S.-Canada Power System Outage Task Force, (2004) , -(sf 190), Erişim Tarihi 14/11/2022 https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

Ünal, A. (2012). ABD İncelemesi. *Siber Güvenlik Raporu.* İstanbul Bilgi Üniversitesi, Bilişim Ve Teknoloji Hukuku Enstitüsü *(*sy.14).

Varlık, Ergün (2017, 25 Mart) "Trump'dan devrim gibi karar" https://siberbulten.com/uluslararasi-iliskiler/trumpdan-devrim-gibi-karar-her-bakanlik-kendi-siber-guvenliginden-sorumlu/

Varon, Sabi (2009), Ortadoğu'da Medya Savaşları, Erişim Tarihi 15.05.2022.

Wikipedia, "Honker Union", (2009), (Erişim 15.06.2022) https://en.wikipedia. org/wiki/Honker_Union

World Economic Forum, (2020) "WEF Global Risk Report", Erişim 10/05/2021, https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf