T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANABİLİM DALI

SİBER SALDIRILARIN EKONOMİK BOYUTU

YÜKSEK LİSANS TEZİ

İbrahim ÖZKAN

Tez Danışmanı
Prof. Dr. Cüneyt KOYUNCU

Bilecik, 2019
10166058

T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANABİLİM DALI

SİBER SALDIRILARIN EKONOMİK BOYUTU

YÜKSEK LİSANS TEZİ

İbrahim ÖZKAN

Tez Danışmanı
Prof. Dr. Cüneyt KOYUNCU

Bilecik, 2019
10166058

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ	SOSYAL BİLİMLER ENSTİTÜSÜ YÜKSEK LİSANS TEZ SAVUNMA SINAVI JÜRİ ONAY FORMU	BŞEÜ-KAYSİS Belge No	DFR-172
		İlk Yayın Tarihi/Sayısı	03.01.2017 / 28
		Revizyon Tarihi	
		Revizyon No'su	00
		Toplam Sayfa	1

Öğrencinin Adı Soyadı: İbrahim ÖZKAN

Anabilim Dalı : İktisat

Programı : Tezli Yüksek Lisans

Tez Danışmanı : Prof Dr. Cüneyt KOYUNCU

Tezin Özgün Adı : Siber Saldırıların Ekonomik Boyutu

Tezin İngilizce Adı : Economic Dimension Of Cyber Attacks

Tez Savunma Sınavı Tarihi: 29 / 07 / 2019

Yukarıda bilgileri verilen tez çalışması ilgili EYK kararıyla oluşturulan jüri tarafından OY BİRLİĞİ /~~OY ÇOKLUĞU~~ ile İktisat Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	*İmza*
Tez Danışmanı: Prof Dr. Cüneyt KOYUNCU	
Üye Prof Dr. Jülide Yalçınkaya Koyuncu	
Üye : Dr. Öğr. Üyesi Yüksel Olsak	
Üye :	
Üye :	

ONAY

Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun ..... / ..... / 20..... tarih ve ... .../... ... ... sayılı kararı.

İMZA/MÜHÜR

BEYAN

Siber Saldırıların Ekonomik Boyutu adlı yüksek lisans tezinin hazırlık ve yazımı sırasında bilimsel ahlak kurallarına uyduğumu, başkalarının eserlerinden yararlandığım bölümlerde bilimsel kurallara uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, tezin herhangi bir kısmını Bilecik Şeyh Edebali Üniversitesi veya başka bir üniversitedeki başka bir tez çalışması olarak sunmadığımı beyan ederim.

İbrahim ÖZKAN

12.07.2019

ÖN SÖZ

Bu tezin yazılması aşamasında en büyük teşekkürü borçlu olduğum, değerli yorumlarıyla bana bir bakış açısı kazandıran, her aşamada yardımlarını esirgemeyen, danışman hocam Prof. Dr. Cüneyt KOYUNCU 'ya değerli katkı ve emeklerinden dolayı teşekkürlerimi ve saygılarımı sunarım. Tez savunma sınavımda beni sabırla dinleyen jüri üyelerime de ayrıca teşekkürlerimi sunarım.

Ders aşamasında bana konu ve kaynak önerilerinde bulunan değerli bilgilerinden istifade ettiğim, Prof. Dr. Aykut EKİNCİ 'ye, Dr. Öğr. Üyesi Resül YAZICI' ya, Doç. Dr. İsmail Hakki İŞCAN' a, Doç. Dr. Necati ÇİFTÇİ 'ye ve Doç. Dr. Ceyhun HAYDAROĞLU hocalarıma teşekkürlerimi sunarım.

Tezin teknik boyutu itibariyle kurslarına katılmış olduğum Bilecik Şeyh Edebali Üniversitesi Endüstriye Dayalı Mesleki Eğitim Merkezine ve Yüksek Mühendis Rıdvan ÖZDEMİR hocama paylaştığı değerli bilgilerden dolayı teşekkürlerimi sunarım.

Son olarak ders aşamasından tez aşamasına kadar ilk günden itibaren birbirimize destek olduğumuz değerli dostlarım Gürkan DANIK ve Eray YILDIZ 'a teşekkürlerimi sunarım.

İbrahim ÖZKAN

…/…/…

ÖZET

Gelişen iletişim teknolojileri her zaman ilk olarak savaş alanlarında denenmiştir. Almanların meşhur Enigma, şifreli telsiz iletişim ağı iletişim güvenliği olgusunu bizlere hatırlatmaktadır. Devamında İngiltere tarafından çözülen bu sistemin maliyeti Almanların İngiltere cephesini kaybetmesine kadar gidecek ağır sonuçlar doğurmuştur. Tarihte örnekleri bol olmakla beraber iletişim güvenliği ve bilgi güvenliğinin sonuçları arasında mutlaka ekonomik bir boyut bulunmaktadır.

Günümüzde bilişim sistemleri ekonomide internet bankacılığı, online pazarlar, üretim yönetimi, askeri alanlarda ve savunma yatırımlarında yer edinmiştir. Bu doğrultu da bilişim teknolojilerinin getirdiği kolaylıkların yanında. Bilgi güvenliğinin de önemi artmıştır ve geçtiğimiz yüzyılda siber saldırılar ciddi ekonomik zararlara yol açmıştır. Bunu keşfeden devletler siber savunma stratejileri geliştirmişlerdir. Savunma bütçe ve strateji eylem planlarında siber güvenliğe yer ayırmaya başlamışlardır. Son yıllarda teknolojik adaptasyonun artması ile birlikte de siber saldırıların ekonomik boyutu giderek şiddetini arttırmış ve siber savaşları doğurmuştur. Ayrıca günümüzde gerçek hayatta karşımıza çıkan vekalet savaşları durumu siber dünyada da geçerli olduğundan, siber savaş ve saldırı ayrımı yapmak pek mümkün değildir. Her iki grup saldırı da birbirleri ile ilişkilidir. Siber saldırı ve siber savaşların ekonomik etkilerinin hesaplanması yönünde henüz bir çalışma mevcut değildir. Araştırmalarımız esnasında bu konuda dünyaca yetkin kurum, kuruluş ve firmaların ellerindeki verilerin siber saldırıların ekonomik etkilerini, ekonometrik analizlerle gerçeğe daha yakın olarak hesaplamak için henüz yeterli olmadığını söyleyebiliriz. Bu sebeple çalışmamızda siber saldırıların ekonomik ilişkilerini ve etkilerini vurgulamaya, bu ekonomik etkilerin ileride yeterli veri ve anlayış oluştuğunda yapılacak çalışmalarda gerçeğe daha yakın olarak hesaplanabilmesi için bir yaklaşım, yöntem ve bakış açısı kazandırmaya gayret ettik.

Anahtar Kelimeler: Siber Güvenlik, Siber Savaşlar, Hacking, Bilişim Güvenliği, Bilişim Ekonomisi, Endüstriyel Casusluk, Siber İstihbarat

ABSTRACT

Developing communication technologies have always been first tested in battlefields. The famous German Enigma reminds us of the concept of encrypted wireless communication security. The cost of this system, which was subsequently solved by England, had severe consequences that would go on until the Germans lost the British front. Although there are plenty of examples in history, there is an economic dimension between the results of communication security and information security.

Nowadays, information systems have taken place in internet banking, online markets, production management, military fields and defense investments in the economy. This is in addition to the convenience of information technology. Information security has also increased in importance and in the last century cyber attacks have caused serious economic damage. States that have discovered this have developed cyber defense strategies. They have begun to devote cyber security to their defense budget and strategy action plans. With the increasing technological adaptation in recent years, the economic dimension of cyber attacks has gradually increased its severity and has caused cyber wars. Furthermore, it is not possible to differentiate between cyber warfare and attacks as the power of attorney wars that we face in real life today is also valid in the cyber world. Both groups are associated with each other to attack. There is no study on the economic effects of cyber attacks and cyber wars. During the course of our research, we can say that the data at the hands of institutions, organizations and companies which are competent in this field is not yet sufficient to calculate the economic effects of cyber attacks more accurately with econometric analyzes. Therefore, in our study, we have tried to emphasize the economic relations and effects of cyber attacks and to provide an approach, method and perspective to calculate these economic impacts in the future when sufficient data and understanding is formed.

Keywords: Cyber Security, Cyber Wars, Hacking, IT Security, IT Economics, Industrial Espionage, Cyber Intelligence

İÇİNDEKİLER

BİRİCİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

İKİNCİ BÖLÜM

SALDIRI ARAÇLARI

ÜÇÜNCÜ BÖLÜM

ÖRNEK OLAYLAR

KISALTMALAR

AB:	Avrupa Birliği
ABD:	Amerika Birleşik Devletleri
ARGE:	Araştırma Geliştirme
CIA:	Merkezi Haber Alma Teşkilatı
CPU:	Merkezi İşlemci Ünitesi
DDOS:	Dağıtık Hizmet Dışı Bırakma
DOS:	Hizmet Dışı Bırakma Denial Of Services
EDMEM:	Endüstriye Dayalı Mesleki Eğitim Merkezi
FBI:	Federal Soruşturma Bürosu
GPS:	Küresel Konumlama Sistemi
GPU:	Grafik İşlemci Ünitesi
HEX:	On Altılık Sayı Sistemi
IMF:	Uluslar Arası Para Fonu
INTERPOL:	Uluslar Arası Polis Teşkilatı
IP:	İnternet Protokolü
KGB:	Rus İstihbaratı
MIT:	Massachusetts Teknoloji Enstitüsü
MITM:	Ortadaki Adam Saldırıları
MİT:	Milli İstihbarat Teşkilatı
MS-DOS:	Microsoft Disk İşletim Sistemi
NATO:	Kuzey Atlantik Paktı
NSA:	Ulusal Güvenlik Ajansı
PENTEST:	Sızma Testi

PLA:	Halkın Kurtuluşu Ordusu
PLC:	Programmable Logic Controller
RTÜK:	Radyo Televizyon Üst Kurulu
SCADA:	Supervisory Control And Data Acquisition
SEA:	Syrian Electronic Army
SEO:	Arama Motoru Optimizasyonu
SOM:	Siber Olaylara Müdahale
TDK:	Türk Dil Kurumu
USCYBERCOM:	Amerika Siber Komutanlığı
vb.:	Ve Benzeri
vs.:	Vesaire
WB:	Dünya Bankası
WTO:	Dünya Ticaret Örgütü

TABLOLAR LİSTESİ

GRAFİKLER LİSTESİ

ŞEKİLLER LİTESİ

GİRİŞ

Siber güvenlik ve siber savaşlar geleneksel savaş yöntemlerini geride bırakarak çağımızın yeni nesil savaş yöntemleri arasında yerini almıştır. Bunda giderek şiddetini arttıran siber saldırıların etkisi göz ardı edilememektedir. İnternetin ilk olarak askeri alanda ABD de haberleşme teknolojisi ile doğuşundan sonra sivil alanda kullanımı ile birlikte dünyanın ekonomik ve kültürel yapısı giderek bilişim merkezli olarak değişmiştir. Bu değişim internetin aksine, ilk olarak sivil kullanıcıların bilişim teknolojilerini saldırı aracı olarak veya sabote aracı olarak kullanmasıyla başlamıştı.

Sonrasında gelişen süreçte devletler siber güvenliğin önemini kavramış ve buna yönelik savunma yatırımları ve savaş stratejileri geliştirmeye başlamışlardır. Siber saldırıların yerini devlet düzeyinde olan siber savaşlar almıştır. Fakat bu olguya tezat bir şekilde siber saldırılar da önemini yitirmemiştir. Çıkışı bireyler bazında olan siber saldırıların aktörlerinin sayıları devletlerin siber komutanlıkları ya da Siber Olaylara Müdahale (SOM) kurumlarının çalışanlarından fazladır. Bu durum siber saldırı örneklerinin siber savaş örneklerine göre daha sık görülmesine neden olmaktadır. Fakat siber saldırılar sık görülmelerine rağmen etkileri siber savaşları aratmayacak derecede yıkıcı olabilmektedir. Ekonomik boyutları açısından bir siber saldırının geleneksel silahlara oranla çok daha fazla ekonomik zarar verdiği günümüzde bilinen bir gerçektir. Bu zararı gözler önüne sermek açısından yakın geçmişte ciddi ekonomik sonuçlar doğuran ve literatüre mal olmuş siber saldırı örnekleri ve siber savaş örneklerine bu çalışmada yer verilmiştir. Ayrıca akıllardaki soru işaretlerine yanıt olması açısından saldırı metodolojisi ve saldırı teknikleri hakkında kavramsal açıdan ince detaylara da yer verilmiştir. Hacking ve siber güvenlik alanında otorite olmuş kaynaklardan faydalanılarak siber saldırıların teknik ve ekonomik boyutları yorumlanmaya çalışılmıştır. Çalışma yöntemi olarak literatür taraması yöntemi kullanılmış ve literatürdeki önemli kaynaklar taranarak elde edilen bilgilere içerikte yer verilmiştir.

BİRİCİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

1.1 SİBER KAVRAMI

Siber kavramı, kurucusu El Cezeri olarak kabul gören sibernetik veya diğer adıyla robot biliminden kısaltma ön eki olarak gelmektedir. Sibernetik Türkiye Bilim Terimleri Sözlüğünde şu şekilde tanımlanır: *"İnsan beyninin oluşturduğu biyolojik süreçler ile her türlü makine veya sistem tarafından yürütülen teknik süreçlerin benzerlik ve farklılıklarını inceleyen ve bu süreç akışlarını ortak temel ilkelere bağlamayı hedefleyen bilim dalı, güdümbilim"*(www.tubaterim.gov.tr, 1.07.2019). Günümüzde ise daha çok sanal erişim veya sanal yaşam olarak kullanılmaktadır (Şahinaslan, 2013, s:3). Siber kelimesi, dil bilimsel açıdan bilgisayar veya bilgisayar ağlarını ilgilendiren ya da içeren kavram veya varlıkları tanımlamak için kullanılan bir kelimedir (Eren, 2017, s: 19). Ayrıca siber kelimesi günümüzde sıkça bilişim anlamında kullanılmaktadır.

1.1.1 Siber Uzay

İngilizce Cyberspace olarak geçen kelimenin Türkiye Bilim Terimleri Sözlüğündeki tanımı şu şekildedir: Bilgisayarlar, bilgisayar ağları ve kullanıcılarının oluşturduğu sanal topluluk(www.tubaterim.gov.tr, 1.07.2019). Siber Uzay terimi ilk kez Amerikalı bilim-kurgu yazarı William Gibson tarafından, 1982 yılında "Burning Chrome" adlı hikâye kitabında kullanılmıştır (Çifci, 2017, s:3).

1.1.2 Siber Saldırı Ve Siber Savaş

Siber uzayın imkânlarını kullanarak bilgi çalma, değiştirme bilişim sitemlerinde tahribata yol açma veya aksatmaya neden olan her türlü girişim, siber saldırı olarak adlandırılabilir. Siber savaş ise bu eylemlerin devlet eliyle veya devletler boyutunda yapılması demektir. Siber savaş konusunda kafaları en çok karıştıran noktalardan birisi

de zaman zaman siber savaşçılar yani devlet tarafından desteklenen hackerlar veya hacker grupları tarafından başka ülkelere saldırı olduğunda, bunu siber savaş olarak adlandırıp adlandırmama konusudur. Bahsi geçen durum da, tıpkı gerçek hayatta olduğu gibi siber uzayda vekâlet savaşları stratejisinin izlenmesi söz konusudur. Ülkeler çoğu zaman uluslararası kanunlarla muhatap olmamak için bu tür çatışmaları gruplar üzerinden yürütürler. Bir siber savaşçı gurubunun başka bir ülkeye saldırması da aslında bir tür siber savaştır.

1.2 HACK KAVRAMI

Hack kelimesi İngilizcede, ilk anlam olarak bir bıçakla veya baltayla kesmek doğramak manasında kullanılmaktadır. Bizim kültürümüze göre değerlendirecek olursak yontmak şekillendirmek gibi bir anlamı ihtiva eder. Bunun bilişim kültüründeki kökenleri ise kısa yollar bulmak işlemleri kestirmeden yapmak anlamında kullanılmıştır.

> *Bilgisayarların ilk örnekleri bir oda büyüklüğünde devasa makinelerdi ve bu makinelerin işleyiş şekilleri günümüz bilgisayarlarından oldukça zordu. "Amerika Birleşik Devletleri'nde bulunan Massachusetts Institute of Tecnology (MIT)'de bir grup araştırmacı bilgisayarları daha etkin kullanabilmek için kısa yollar oluşturdular. Akabinde, 1969 yılında tarihin ilk ve en büyük Hacking olayı denilebilecek Dennis Ritchie ve Ken Thampson adında iki dâhinin Bell Laboratuvarlarında Linux ve Windows gibi işletim sistemlerinde hala büyük etkisi olan "C" dilini geliştirmeleri olayı gerçekleşti. Daha sonra bu ikili ilk işletim sistemi olan UNIX işletim sistemini yazdılar* (Elbahadır, 2017:11).

Bilgisayar korsanlarının(Hacker) ilk örneklerinden olan ve birkaç kez çeşitli bilişim suçlarından ceza aldıktan sonra beyaz şapkalı Hacker olmaya karar veren ünlü bilgisayar korsanı Kevin D. Mitnick bu konu hakkında şunları söylüyor*: O zamanlar, daha etkili programlar yapmak ya da gereksiz basamakları atlayıp işi daha hızlı yapabilmek için zamanının çoğunu bilgisayarları ve yazılımları kurcalamakla geçiren kişilere korsan derdik* (Mitnick & Simon, 2017:xi). Mitnick 'in söyledikleri hack kavramının türetildiği ve değiştiği sürece şahitlik etmiş olması ve bizzat kendisinin hacking ve hacking ile mücadele cephesinin her iki tarafında da yer almış olması açısından önemlidir.

Hack kavramı medyada genellikle siber suçluların yaptıkları eylemler olarak tanımlanır. Bu tanım yanlış olup, toplumda da yanlış bir algıya yol açmıştır (Altınkaynak, 2017 :1). Bütün bunlar ve bu kavram üzerine yazılan daha pek çok destekleyici yorumlar doğrultusunda bugün günümüzde sosyal medyada Life Hack şeklinde kullanılan bir

kavramdan örnek vermek akıllardaki soru işaretlerine cevap olacaktır. Life hack hayatı hacklemek problemlere akılcı pratik çözümler bulmak anlamında kullanılmaktadır. Örnek vermek gerekirse bir konserve kutusunu yumurta pişirme kabı olarak kullanmak life hack'in en basit örneklerindendir. Hack kavramının kullanımına ilişkin bir diğer örnekte günümüzde iş kültüründe pazarlama ve büyüme stratejileri altında yer edinmiş olan Growth Hacking kavramıdır. Growth Hacking, yeni nesil pazarlama ve reklam araçları olan dijital reklamcılık, sosyal medya reklamcılığı ve Search Engine Optimizasyon (SEO) arama motoru optimizasyonu gibi teknikleri kullanarak etkin bir şekilde pazarlama çalışmaları yürüten, bir tür pazarlama ve büyüme stratejisidir.

Bir şeyleri amacı dışında kullanmak problemlere akılcı pratik çözümler bulmak bütün bunlar hack kavramının kapsamındadır. Fakat bu çözümlerin sıklıkla bilgisayar programlarının ve bilişim sistemlerinin prosedürlerini atlatmak ve işleyişine müdahale ederek normal şartlar altında elde edilmemesi gereken, bilgiler ve elde edilmemesi gereken kazanımlar elde etmek, bilgi hırsızlığı için kullanmak gibi kötü örnekleri ile gündeme geldiği için bu kavramın adı kötüye çıkmıştır.

1.3 BİLGİSAYAR KORSANI (HACKER) KAVRAMI

Hacker kavramı açıklamış olduğumuz hack olayını icra eden kimse anlamındadır. Örnek vermek gerekirse hack bölümünde anlatmış olduğumuz "C" dilinin ve Unix işletim sisteminin yazarları Dennis Ritchie ve Ken Thampson da birer hackerdır, haberlerde sıkça adlarını duyduğunuz çeşitli amaçlarla çeşitli hedeflere siber saldırılar gerçekleştiren, gizli bilgileri çalan, bilişim sistemlerini çökerten, medyada sürekli hayalet gibi korkutucu ve gizemli bir şekilde sunulan kişilerde hackerdır. Çözümün veya problemin bir parçası olmayı seçmiş olmaları kavram açısından bir şeyi değiştirmemektedir temelde yaptıkları iş aynıdır.

TDK 'da ise hacker kelimesinin Türkçe karşılığı olan bilgisayar korsanı şu şekilde tanımlanmaktadır: "Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse" (http://sozluk.gov.tr, 2019). Bu tanımlamada, tüm bilgisayar korsanlarının bilişim teknolojilerini kötü niyetlerle kullandıkları vurgusu öne çıkmaktadır. Bu kişilerin, daha çok olumsuz örneklerle gündeme gelmiş olmalarının, bu vurguda payı büyüktür. Ancak

gerçekte hacker kavramında öne çıkması gereken, bilgisayar ve haberleşme teknolojilerini kullanmada üstün yetenekli ve eğitilmiş kişiler olduklarıdır (MERAL, 2015:10).

Teknolojinin gelişimi ve siber dünya ile gerçek dünya arasındaki çizginin giderek inceldiği günümüz dünyasında, Siberpunk kültürünün ilk örneklerinden olarak ortaya çıkan, Matrix Felsefesinin yaratıcısı William Gibson, "Matrix Avcısı" adlı romanında bilgisayar korsanlarından "büyücü" olarak bahseder. Günümüz dünyasında böyle bir bağıntı belki hâlâ anlaşılamayabilir. Fakat durumu açıklamak için oldukça yerinde bir mecazdır, şimdilik! Dünya üzerinde her kültürde, her dinde büyü kavramı mevcuttur, kabile toplumlarından tutun da en gelişmiş toplumlara kadar ne olduğu bilinir. Evrensel bir kavramdır. Evrenin gizemli yasalarını kullanarak hayata müdahale etme, evrenin ve hayatın işleyişine müdahale etme anlamındadır. Bu şekilde düşündüğümüzde bilgisayar korsanları gerçekten de geleceğin büyücüleridir. Diğer insanların anlamadığı bir takım tekniklerle sistemlerin işleyişine müdahale ederler. Ve bu birçok kişi için sihir gibi mucizevidir. Teknolojinin kendisi de zaten böyledir. Bu konuda ünlü İngiliz mucit ve bilimkurgu yazarı Arthur Charles Clarke'ın sözü akıllara gelmektedir:" Yeterince gelişmiş bir teknoloji, sihirden ayırt edilemez." Gene aynı doğrultuda, bir zamanlar dünyanın en çok aranan hackerı olan Kevin D. Mitnick, Aldatma Sanatı kitabında şunları söylemektedir: "Erken yaşlarda ortaya çıkan başka bir kişisel ilgi de sihirbazlık yapmaya olan hayranlığımdı. Bir numaranın nasıl yapıldığını bir kez öğrendikten sonra, iyice ustalaşana kadar durmaksızın üzerinde çalışıyordum. Gizli bilgileri elde etmenin eğlencesine, kısmen sihirbazlık sayesinde vardım" (Mitnick & Simon, 2017:x).

Hackerlar bu yönden illüzyon ustalarıdır, diğer insanların görmediği detayları görür, bunları sistemi istismar etme veya onarma doğrultusunda kullanırlar. Ve gerektiği yerde sosyal mühendisliği de bir hacking aracı olarak çok iyi düzeyde kullanıp, insanlarda her şey yolundaymış algısı yaratarak almak istedikleri bilgileri alırlar.

Tüm bu anlamlandırma karmaşasının çözümü olarak hacker çeşitleri ortaya çıkmıştır bunlara değindiğimizde aklınızdaki kavrama ilişkin soru işaretleri cevap bulacaktır.

1.3.1 Siyah Şapkalı Hackerlar (Black Hat)

Siyah şapkalı hackerlar, şapkanın adında da anlaşılabileceği gibi kötü niyetli ve karanlık kişilerdir (Çıtak, 2018:3) Sahip oldukları bilgi ve yetenekleri zarar vermek için kullanmaktadırlar. Bu zarar çoğu zaman parayla karşılık bulur (Altınkaynak, 2017:2). Yaptıkları işler yasa dışı ve insani değerlere aykırı olduğundan, pek gün yüzüne çıkmak, bilinmek istemezler, kendilerini gizlerler. Motivasyonları tamamen para veya eğlencedir, hiçbir etik kaygıları yoktur. İnterneti ve bilgisayarı para kazanma aracı olarak görürler. Para karşılığında veya eğlence amaçlı olarak akıllarına gelebilecek her şeyi hiç düşünmeden yapabilirler. Bir terör örgütüne para karşılığı hizmet vermek, bir mafya örgütü, bir istihbarat örgütü ya da parayı veren herhangi birine hizmet vermek onlar için sorun teşkil etmez. Bu tür kişiler genelde siber suçlarla mücadele eden kurum ve kuruluşların radarına takılmamak için Darknet denilen derin ağ üzerinden veya CSS(Closed Shell System) şifrelenmiş(kriptolu) ağı üzerinden internette dolaşırlar. Bunca güvenlik önlemi almalarının yegâne sebebi, en başından beri değindiğimiz üzere her türlü yasa dışı ticaret ve işin bu ağlar üzerinden organize ediliyor olmasıdır. Ödemeler ise merkezi olmayan dağıtık bir sisteme sahip olan kripto paralar üzerinden yapılır. Ve dağıtık yapısından dolayı bu transferlerin izi sürülemez.

1.3.2 Beyaz Şapkalı (White Hat) Hackerlar

Bir diğer adı siber güvenlik uzmanı veya etik hackerdır. Bilişim sistemleri konusunda ileri derece de bilgi sahibi olup, bu bilgiyi yasal çerçeve de kullanan kişilerdir. World Wide Web (www) sistemini ve hiypertext olarak bilinen http sistemini, hayatımıza kazandıran web ’in babası Tim Berners-Lee ve Linux’un mucidi Linus Torvalds beyaz şapkalı hackerdır (Kara, 2013:13). Siyah şapkalı hackerlar ile aralarındaki fark bir çilingir ve hırsız arasındaki farka benzetilebilir. Beyaz şapkalı hacker fikrinin temeli, aslında temelde askeri alanda kullanılırken daha sonra iş dünyasında, strateji ve denetim gerektiren hemen her alanda kullanılmaya başlayan, sonrasında da “etik hacker” kavramı ile bilişim dünyasında vücut bulan, kırmızı takım kavramından gelmektedir. Kırmızı takım mantığı temelde bir tatbikat üzerine kuruludur. Askerler iki gruba ayrılırlar savunan taraf mavi takım ve saldıran taraf kırmızı takım. Mavi takım birliğin flamasını korumaya

kırmızı takım ise onu ele geçirmeye çalışır. İş dünyasında bu flama bir ihale, anlaşma, strateji ve rekabet gerektiren başka herhangi bir şey olarak vücut bulurken, bilişim alanında bilişim sistemlerinde muhafaza edilen verilerdir. Ünlü Çin Savaş Filozofu Sun-Tzu Savaş Sanatı adlı eserinde bu tür stratejilere ilişkin şunları söylemiştir: "İyi savaşçılar düşmanın ayağına gitmezler, düşmanın kendi ayaklarına gelmesini sağlarlar." Sun-Tzu savaş sanatı felsefesi askeri alandan tutun da iş dünyası ve bilişim alanına kadar pek çok alanda strateji kurma açısından etkin olarak kullanılmaktadır.

Hacking kavramı her ne kadar MIT Laboratuvarlarında can bulmuş olsa da toplumda ki karşılığı çok daha fazla olmuştur. Bilişim sistemlerinin temellerinin atıldığı zamanlarda hacking eğitimi veren kurumsallaşmış yapılar olmadığı için, gününüz siber güvenlik uzmanlarının çoğu kendisini yetiştirmiştir. Hatta bir çoğu da Mitnick gibi veya Türkiye'nin ilk hacker'ı olan Tamer Şahin gibi siyah şapkalı hacker olarak başlayıp sonrasında siber suçlarla ilgili yasal düzenlemeler ve otoritelerin kurulması ile beyaz şapka veya etik hacker olarak hizmet vermeye devam etmişlerdir. Günümüzde artık bu tür eğitimler veren kurum ve kuruluşlar mevcuttur. Pek çok üniversite ve eğitim kurumu etik hackerlık eğitimlerini müfredatlarına katmışlardır.

1.3.3 Gri Şapkalı (Gray Hat) Hackerlar

Siyah ve beyaz şapka arasındaki ince çizgidedirler (Çıtak, 2018:5).Yasallık sınırında olup, yerine göre siyah veya beyaz tarafı seçerler (Bülbül & Bingöl, 2017:16).Normal şartlar altında etik hackerların bir bilişim sisteminin güvenliğini sağlamak için sistem sahipleri ile aralarında antlaşmaları vardır. Fakat gri şapkalı hackerlar sistem sahiplerinin bilgisi dışında sistemleri analiz ederler ve buldukları zafiyetleri(hata ve açıkları) keyiflerine göre kullanırlar. Buldukları zafiyeti kullanarak siyah şapkalı hackerlar gibi bu durumdan çıkar elde etmek için de kullanabilirler. Veya bu durumu sistem sahiplerine bildirip karşılığında bir ödül de umabilirler. Fakat sistem sahipleri, bilgileri olmaksızın sistemlerinin incelenmesinden hoşnut olmayacakları için saldırgan davranabilirler. Osmanlı Bankası örneğinde olduğu gibi.

1.3.4 Hactivistler

Eylemci (Aktivist) kelimesinden türetilmiş bir kavramdır. Genel olarak toplumda yanlış buldukları aksaklıkları ve doğru olmadığını düşündükleri şeyleri değiştirmek amacıyla, eylemler düzenleyen kimselerdir. Bunun siber âlemde hayat bulmuş hali ise hactivizm kavramıdır. Hactivist hackerların yada hacktivist hacking gruplarının genel motivasyonları, toplumda veya ülkelerin izledikleri politikalarda yanlış gördükleri şeyleri değiştirmek üzerinde kuruludur. Bunun birçok çeşidi mevcuttur. Politik bir yapıda olduklarından, aralarında milliyetçi duygularla hareket edenler olduğu gibi toplumsal duygularla hareket edenlerde vardır. Örnek vermek gerekirse RedHack kendilerini kırmızı şapkalı hacker olarak tanımlarlar (Kara, 2013:14). Bu tanımda sahip oldukları toplumcu sosyalist siyasi görüşlerinin elbette etkisi vardır. Ülkemizdeki diğer hactivist gruplar Ayyıldız Team, Cyber-Warrior ve Türk Hack Team gibi gruplar ise genel olarak kendilerini vatansever hackerlar olarak tanımlarlar. Yaptıkları eylemler ise politik görüşleri ile paralellik göstermektedir. Dünya çapında örnek vermek gerekirse Hactivizm Wikileaks veya Anonymous'un yaptıklarına, hacktivist ise Julian Assange gibi kişi ve Anonymous gibi gruplara denir (Çıtak, 2018:7).

1.3.5 Phreakerlar

Terimin kökeni Phone(Telefon) Hacker kavramından gelmektedir. Telefon ve telekomünikasyon sistemlerini hackleme üzerine uzmanlaşan kişilerdir. 70'li yıllarda Cap'ın Crunch adıyla satılan mısır gevreği kutularından çıkan düdükle, 2600 hertzlik telefon çevir sesi çıkarabileceğini keşfedip, bunu kullanarak ücretsiz görüşmeler yapan John Draper, ilk phreaker örneklerindendir (Elbahadır, 2017:9). John Draper bu olaydan sonra, Kaptan Crunch olarak anılmaya başlanmıştır. Aynı zamanda Kevin Mitnick' te hacking maceralarına ilk başladığı zamanlarda, telekomünikasyon firmaları ve sistemleri üzerine, yoğun olarak çalıştığını belirtmektedir.

Telefon sistemleri ve internet birbirine sıkı sıkıya bağlıdır. Günümüzde akıllı telefonların çıkması, telefon ve bilgisayar arasındaki farkı iyice ortadan kaldırmıştır. Bugün cebimizde taşıdığımız akıllı telefonlar aslında birer avuç içi bilgisayardır. Hepsinin işlemcisi, hatta bazı modellerin ayrıyeten grafik işlemcisi, klavye ve girdiler

için mikrofon, kamera ve dokunmatik ekran, hatta bilgisayarlarda bulunmayan ekstra bazı sensörler de dâhil olmak üzere giriş birimleri bulunmaktadır. Kendilerine özgü işletim sistemleri ve bir bilgisayardan beklenen hemen her işi yapabilmeleri bakımından, günümüz akıllı telefonlarının, tam anlamıyla avuç içi birer bilgisayar oldukları söylenebilir.

1.3.6 Yazılım Korsanları (Cracker)

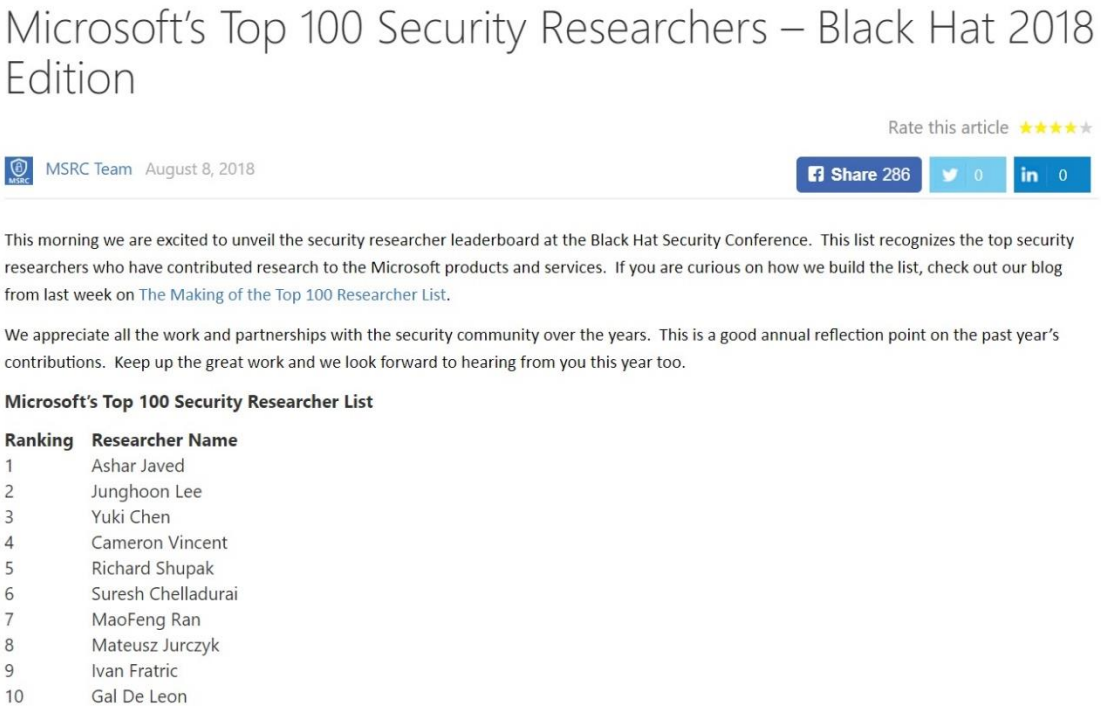
Doksanlı yıllarda kapalı kaynak kodlu yazılımlar, diğer bir deyişle ücretli yazılımların ortaya çıkmasına tepki olarak, bu yazılımları tersine mühendislik yöntemleriyle kırıp, ücretsiz hale getirdikleri kopyalarını internette yayan kişilere verilmiş bir isimdir. İyi düzeyde programlama bilgisine sahip olan bu kişiler, genellikle ücretli programlar üzerine yoğunlaşıp kırdıkları programları ücretsiz olarak dağıtırlar (Bülbül & Bingöl, 2017:17). Günümüzde de halen aktif olarak birçok ücretli yazılımın warez yani kırılmış ücretsiz kopyasını yayımlayan warez siteleri mevcuttur. İlk işletim sistemlerinden biri olan ve Bell Laboratuvarlarında geliştirilmiş olan Unix'i inceleyerek, Linux işletim sistemini ortaya çıkaran Linus Torvalds, bir nevi en iyi cracker örneklerindendir. Fakat buradaki fark Tornvalds Unix'i birebir kopya etmemiştir çalışma sisteminden esinlenerek Linux'u ortaya çıkarmıştır. Tornvalds ve Genel Kamu Lisansı (GNU) projesine destek verenler, tamamen ücretsiz bir işletim sistemi hayata geçirmişlerdir. Crackerların motivasyonları temelde açık kaynak kodlu yazılım savunucuları ile aynıdır, yazılımların ücretsiz ve herkes tarafından ulaşılabilir olması gerektiği düşüncesi.

1.3.7 Hata Avcıları

Bilişim firmaları, hata avcılığı ödül programları düzenlerler. Bu pogramlar, genelde Bug Bounty olarak adlandırılırlar. Buradaki "Bug" terimi sıkça duyduğunuz veya duyacağınız bir terim olup, Türkçe karşılığı "Böcek" demektir. Böceklerin, oda büyüklüğünde olan bilgisayarın ilk örneklerinin devreleri arasına girerek, bilgisayarlara hata verdirdiği zamanlardan kalmıştır. Ve günümüzde de hata anlamında kullanılmaktadır. Microfost, Google, Facebook gibi daha pek çok bilişim firması, bu

programları düzenleyip duyurusunu yaparlar. Ve ilgili kişiler, yani hata avcıları şirketin ürünlerini incelemeye başlarlar. Bir açık bulduklarında bunu şirkete bildirirler. Buldukları hatanın büyüklüğüyle orantılı olarak, bir takım ödüller kazanırlar. Bu ödüller para ödülü olabildiği gibi sembolik ödüllerde olabilir. Verilen ödül bulunan açığın veya hatanın büyüklüğüne bağlıdır. Sonrasında da bu hataları bulup bildiren kişilerden oluşan listeler yayınlanır. Bunun iki amacı vardır: ilk olarak bir nevi şirketin teşekkürüdür, ikinci olarak ta hataları bulan hata avcılarının motive olmasını ve piyasa tarafından tanınarak değerinin bilinmesini sağlar.

Aşağıdaki şekilde Microsoft firmasının 2018 yılı en iyi 100 hata avcısı listesi görülmektedir.



Microsoft's Top 100 Security Researchers – Black Hat 2018 Edition

Rate this article ★★★★★

MSRC Team August 8, 2018

Share 286 | 0 | in 0

This morning we are excited to unveil the security researcher leaderboard at the Black Hat Security Conference. This list recognizes the top security researchers who have contributed research to the Microsoft products and services. If you are curious on how we build the list, check out our blog from last week on The Making of the Top 100 Researcher List.

We appreciate all the work and partnerships with the security community over the years. This is a good annual reflection point on the past year's contributions. Keep up the great work and we look forward to hearing from you this year too.

Microsoft's Top 100 Security Researcher List

Ranking	Researcher Name
1	Ashar Javed
2	Junghoon Lee
3	Yuki Chen
4	Cameron Vincent
5	Richard Shupak
6	Suresh Chelladurai
7	MaoFeng Ran
8	Mateusz Jurczyk
9	Ivan Fratric
10	Gal De Leon

Şekil 1: Microsoft Top 100 Security Researchers

Kaynak: Microsoft, *https://blogs.technet.microsoft.com/msrc/2018/08/08/microsofts-top-100-security-researchers-black-hat-2018-edition/ : 5.7.2019)*

1.3.8 Script Kiddle

Script sözcüğü Türkçe Bilim Terimleri Sözlüğüne göre: Bilgisayarda belirli bir işi gerçekleştirmek için gerekli görev adımları bulunduran betik dili adı verilen özel bir dille yazılmış yönerge program (http://www.tubaterim.gov.tr, 2019) şeklinde tanımlanmıştır. script İngilizce olarak senaryo veya yönerge gibi bir anlam ifade etmektedir. Bilgisayar

programları genelde bir çok modülden oluşur, modül iş parçası olarak tanımlanabilir. Örneğin yemek sepeti gibi bir sipariş programının içerisinde muhtemelen üyelik ve kayıtlar için ayrı bir modül ve üye iş yerlerinin mesafesini hesaplamak için ayrı bir gps modülü yer almaktadır. Yani her iş parçası ayrı bir modülden oluşur ve bunların birleşimi ile bilgisayar programları meydana gelir. Scriptler ise modülün alt birimleridir ve kodlara en yakın yapı oldukları için sıklıkla programlama kodları ile karıştırılırlar. Her script içerisinde kullanılacağı programlama diline özel olarak hazırlanır. Script Kiddle'lar ise başkalarının hazırladığı program parçacıklarını bilişim sistemlerine saldırı yapmak için kullanan kişilerdir. Genellikle çocuk yaşta sayılabilecek bir yaş aralığına sahip odlukları için kiddle eki almış bir terimdir. Script Kiddle'lar hazır program parçacıklarıyla hacking yapmaya çalıştıkları için, aşağılama amacıyla veya eylemlerindeki teknik yetersizliklerini vurgulamak amacıyla diğer hackerlar ve uzmanlar tarafından da kullanılan bir terimdir.

1.3.9 Lamer

Hiçbir bilgisi olmamasına karşın "Ben Hacker'ım " diyerek etrafta gezinen programlama bilgisi olamayan internetten öğrendiği birkaç sıradan işle ün kazanmaya çalışan hacker olma özentisi kişilerdir (Elbahadır, 2017:9). Bu terim hacking kültüründe genelde argo bir hakaret olarak kullanılır. Hack grupları arasında ki çatışmalarda birbirlerine hakaret etmek için genel olarak script kiddle veya lamer terimlerini kullanırlar.

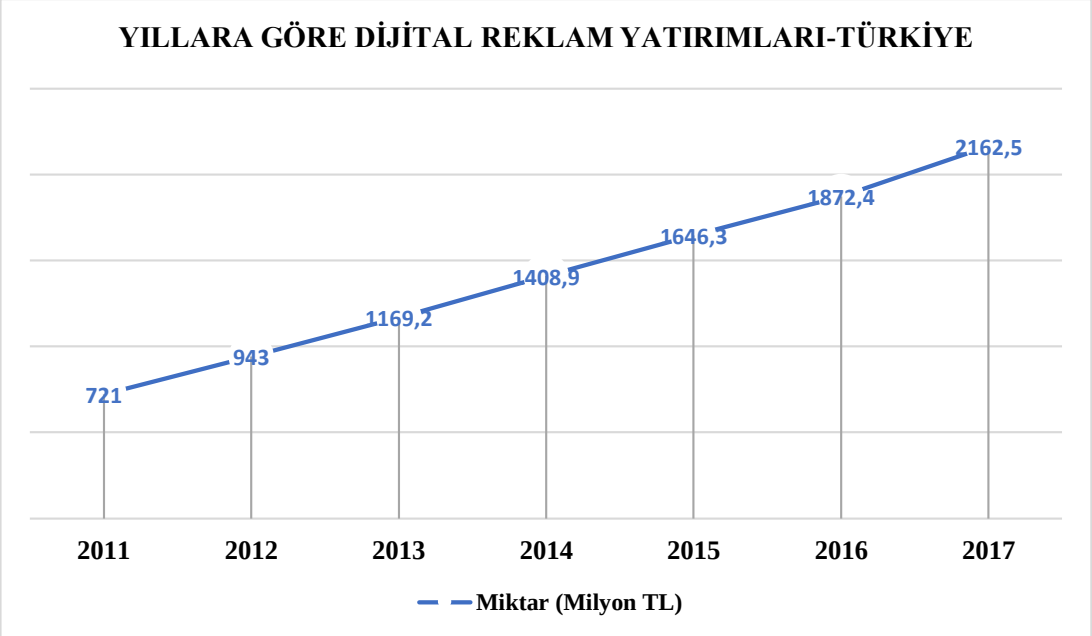
1.3.10 Carderlar

Kredi kartı dolandırıcılığı, pos cihazları veya bankamatik sitemlerine yerleştirdikleri cihazlar ile kart bilgilerini kopyalamak gibi, ödeme sistemleri üzerine uzmanlaşmış kişilerdir. Amaçları siyah şapkalı hackerlar gibi hacking yolu ile para elde etmektedir. Çeşitli hacking yöntemleri ile müşterilerinin kayıtlarını tutan sitelerin veri tabanlarına erişip bu veri tabanlarında kayıtlı olan kart bilgileri üzerinden online alışveriş yaparak satın aldıkları ürünleri paraya çevirmeye çalışırlar. Bu tür alışverişlerini, genelde "cardable" diye tabir edilen, 3d güvenlik sorgulaması gerektirmeyen, yani kredi kartı sahibinin bankaya kayıtlı cep telefonuna bir onay mesajı göndermeyen sitelerden

yapmaktadırlar. Son olarak izlerini kaybettirmek için, ele geçirdikleri kredi kartı bilgilerinin bir kısmını, Darknet gibi karanlık ağlarda satarlar ya da yerine göre ücretsizde dağıtabilirler. Bu bilgileri dağıtmalarındaki amaç, kendilerinden başkalarının da bu kredi kartı bilgilerini kullanmasını umarak izlerinin sürülmesini zorlaştırmaktır.

1.4 SOSYAL MEDYA

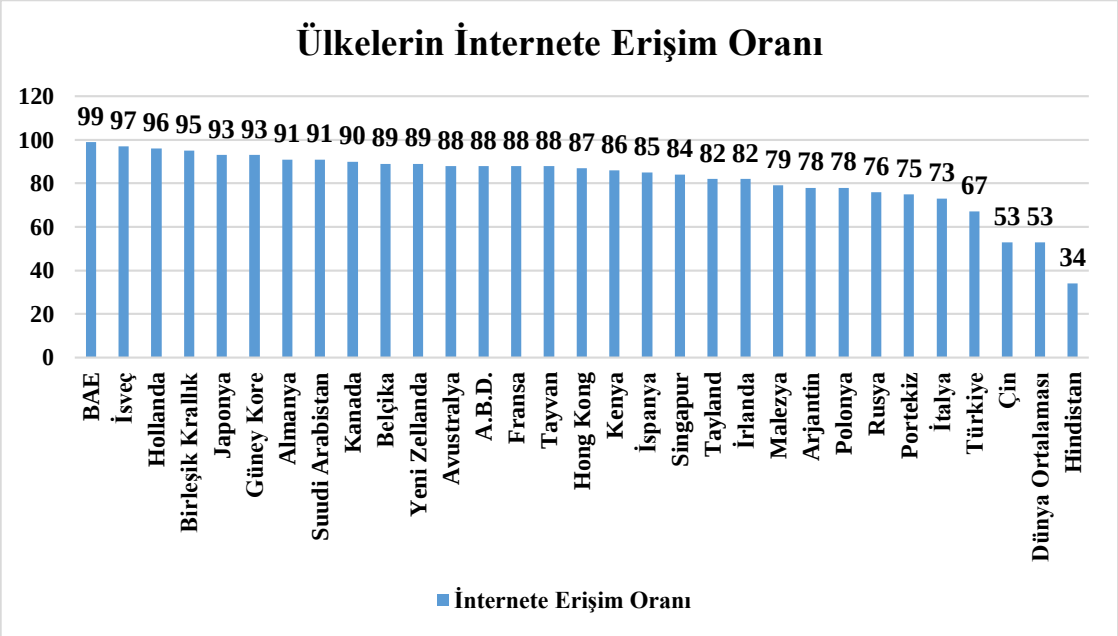
Sosyal medyanın temelleri ICQ ve MIRC gibi temel anlık mesajlaşma uygulamalarıyla atılmıştır. Sosyal medya 99'da Microsoft'un MSN Messenger uygulamasını piyasa sürmesiyle kullanıcılar arasında iyice yer edinmiştir. Devam eden süreçte Mark Zukenberg'in ilk sürümünü üniversite öğrencileri için Harvard Üniversitesi'nin yurdunda 4 Şubat 2004'te "The Facebook" adıyla kurduğu, sosyal medya platformunu, 2006 da tüm dünyaya açmasıyla birlikte sosyal medya akımı çığ gibi büyümüştür. Ardı ardına Twitter, İnstagram, Forsque ve daha pek çok sosyal medya platformu geliştirilmiştir. Ve hepsinin kendisine özgü bir kitlesi oluşmuştur. Sadece Facebook kurulduktan 8 yıl sonra 1,3 milyar üyeye ulaşmıştır. Her gün 350 milyon fotoğraf facebook'a yüklenirken, beğeni tuşuna yaklaşık 6 milyar kez basılmaktadır (Goodman, 2016, s:72).



Grafik 1: Yıllara Göre Dijital Reklam Yatırımları-Türkiye
Kaynak: Veri Kaynağı, IAB Türkiye- Sektörel Araştırmalar,

Gene ülkemiz açısından da reklamcılık sektörünün sosyal medya ve diğer dijital mecralara doğru bir eğilim gösterdiği yukarıdaki şekilde görülmektedir. İnternet reklamcılığının hızlı bir yükseliş göstermesi dikkat çekmektedir.

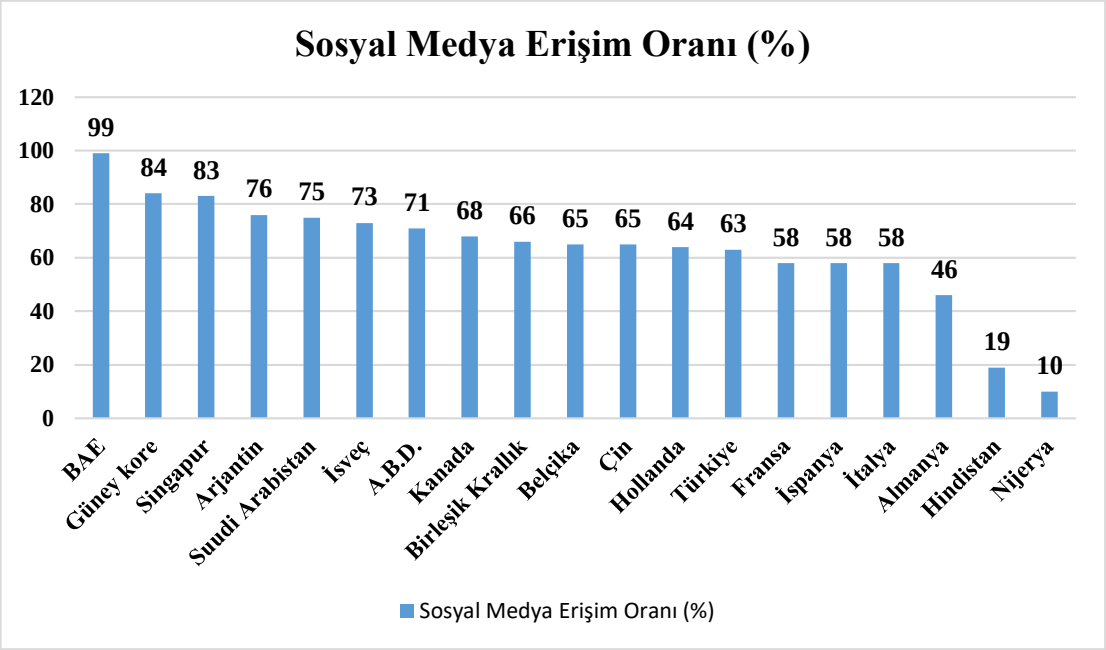
Sosyal medya tam anlamıyla geleneksel medya kanallarının yerini almaya başlamıştır. Kullanım oranları ve sosyal medya ya yapılan reklam yatırımlarını göz önüne aldığımızda, ekonomi cephesinde de karar vericiler bu durumu doğrulamaktadır. Geçmişte siyasi ve ekonomik açıdan medya oldukça önem arz etmekteydi. Reklam ve siyasi destek amacıyla bütün şirketler ve siyasi kuruluşlar, medyada yer almak için çaba sarf ediyorlardı. Günümüzde ise durum tamamen değişmiş durumdadır. Artık siyasi partilerin seçim programlarında, sosyal medya çalışmaları da önemli bir yer edinmiştir. Geçtiğimiz 2019 yerel yönetimler seçimlerini düşünürseniz, partilerin sosyal medya platformları üzerinden ciddi çalışmaları olmuştur. Gene buna benzer çalışmaları, ABD başkanlık seçimlerinde de görmek mümkündür. Aynı şekilde firmalar da ürünlerini pazarlamak için sosyal medya reklamcılığına yönelmişlerdir.



Grafik 2: Ülkelerin İnternete Erişim Oranı

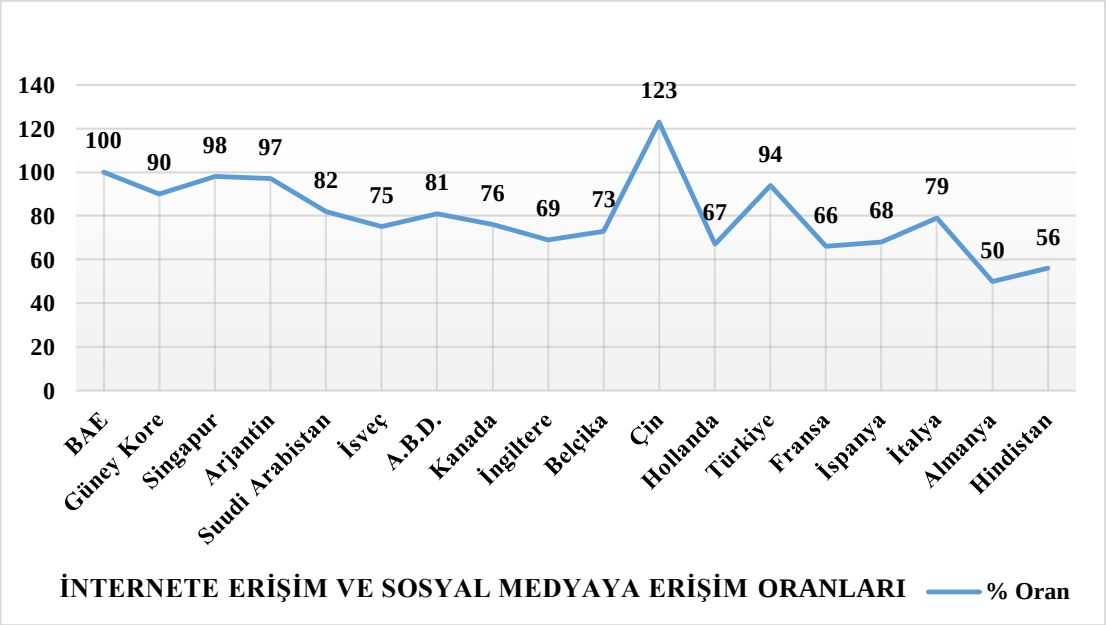
Kaynak: Digital in 2018 Global Overview, verileri kullanılarak tarafımızdan oluşturulmuştur

Grafik 2'de ülkelerin internete erişim oranları görülmektedir. Aşağıda verilen grafik 3'te ise ülkelerin sosyal medyaya erişim oranları verilmiştir. Oranlar genel olarak birbirine yakın olmakla beraber, medyanın ve internetin sıkı bir denetime tabi olduğu Çin özellikle göze batmaktadır.



Grafik 3: Sosyal Medyaya Erişim Oranı
Kaynak: Digital in 2018 Global Overview Verleri Kullanılarak Tarafımızdan Oluşturulmuştur

Birleşik Arap Emirlikleri, internete erişim oranı ve sosyal medya kullanım oranı açısından, her iki grafikte de ilk sırada gelmektedir. İnternet erişimi oranı açısından altıncı sırada yer alan Güney Kore ise, sosyal medya erişim oranı açısından BAE'nin ardından ikinci sırada gelmektedir. Gene bu şekilde liste düzensiz bir şekilde devam etmektedir. Ülkelerin internet erişim oranı sıralaması ile sosyal medya erişim sıralaması değişiklik göstermektedir. Bu sonuç ileride anlayacağımız üzere pek çok açıdan oldukça önemli bir veridir. Bu verileri daha anlamlı hale getirebilmek çabasıyla bahsi geçen ülkelerin internet erişim oranları ile sosyal medya erişim oranları birbirine oranlanarak aşağıdaki grafik 4'elde edilmiştir. Oluşturduğumuz grafik 4'e göre örneğin %99'unun internet erişimi olan BEA'deki kullanıcıların %100'nün sosyal medyaya erişimi bulunmaktadır. Yani BEA'de interneti olan herkes, sosyal medyayı da kullanıyor. Bir diğer dikkat çekici olan ülke ise Çin'dir. Çin nüfusunun internete erişim oranı %53 iken sosyal medya erişim oranı %65 dir. Oransal olarak ta grafik 4'te gösterildiği üzere, Çin'de internete erişebilen her 100 kişiye karşın 123 kişi sosyal medyaya erişebilmektedir. Bu rakamlar matematiksel olarak anlamsızdır. Fakat Çin Hükümeti'nin internet üzerindeki ve sosyal medya üzerindeki baskıcı tutumu göz önüne alındığında durumun bu yasakların delinmesinden kaynaklı olduğu anlaşılmaktadır.



Grafik 4: Ülkelerin internet erişim oranları ile sosyal medya erişim oranlarının % oranı
Kaynak: Grafik 2 ve 3'deki veriler kullanılarak tarafımızdan oluşturulmuştur

Günümüzde sosyal medya, geleneksel medyanın yerini alarak ekonomi de ve ülkelerin siyasetinde önemli rol oynamaktadır. Arap Baharı ismiyle anılan Libya, Mısır ve sonrasında Suriye'nin iç savaşa sürüklenmesine sebep olan olaylar silsilesi, sosyal medya platformlarında başlayıp sokağa taşmıştır. Ülkemizde de yakın geçmişte "Gezi Parkı Olayları" ismiyle anılan, olayların da gene sosyal medya mecralarında başlayıp sokağa taşmış olması, sonrasında bu olaylardan kaynaklı ekonomimizin sıkıntıya girmesinden dolayı ekonomik etkilerini yakinen bilmekteyiz. Günümüzde de gene Fransa'da, sosyal medya mecralarında başlayıp sokağa taşan, "Sarı Yelekliler Hareketi" ismiyle anılan olaylar halen devam etmektedir.

1.4.1 Maslow'un İhtiyaçlar Hiyerarşisinde Medya Ve Sosyal Medya

Geçmişten beri medya, bireyler ve toplumlar için önem arz etmiştir. Tarihte gazetenin ilk olarak nerede ve kimin tarafından çıkarıldığı, tarihçiler tarafından tartışılan bir konudur. Fakat tartışmasız olan, gazetenin çıktığından ve yayıldığından beri, toplumun ilgisini çekmiş olmasıdır. Toplumdaki bireylerin, çevresini ve çevresinde olup biten güncel olayları, bilme ve içinde bulunduğu toplumu anlama isteğine bir yanıt olmuştur.

Medya, Maslow'un beş basamaktan oluşan temel ihtiyaçlar hiyerarşisi piramidinde, fizyolojik ihtiyaçlar dışında kalan dört temel ihtiyaca da hitap etmektedir. Bunlardan ikinci sırada olan "güvenlik ihtiyacını" medya bir nebze karşılamaktadır. Örnek vermek gerekirse, herhangi bir toplumsal tehlike karşısında, bireyler hemen en yakınındaki medya aracını kontrol etmektedir. Hemen, içerisinde bulunduğu toplumla ilgili bilgiler edinip, güvende hissetmek isterler. Veya tersini düşündüğümüzde, bireyler tehlike haberleri aldıklarında, endişeli hissederler ve güvenlik algıları sarsılır. Bu haber alma aracı veya medya aracı, eski zamanlarda gazete iken sonrasında radyo ve televizyon derken günümüzde internetin gelişimi ile sosyal medya olmuştur.

Gene temel ihtiyaçlar piramidinde, üçünü sırada gelen "ait olma" veya "sevgi ve ait olma" ihtiyacına da medya hitap etmektedir. Bireyler, bulundukları topluma aitlik hissederler ve bu yüzden toplumla olan bağlarından birisini oluşturan, onlara yaşadıkları toplumla ilgili bilgiler veren medya, bireylerin aitlik dürtülerini pekiştirdiği için gene önem arz etmektedir. Sonuç itibariyle medyada yer alan kimseler, toplum tarafından sevilen kimselerdir.

Bir diğer temel ihtiyaç ise temel ihtiyaçlar hiyerarşisinde, dördüncü basamakta bulunan "saygı görme ve saygınlık kazanma" ihtiyacıdır. Bu bağlamda da gene medyaya baktığımızda, bazı uç örnekler dışında, genel olarak saygın ve toplum tarafından saygı gören yüzleri görürüz. Bu sadece medyada yer alma anlamında değildir. Medya gelişip topluma mal olduğu zamanlardan bu güne kadar, içinde bulunulan toplum hakkında malumat sahibi olmak ta bir saygınlık göstergesi olarak görülmüştür. Uç örneklere gelince, onlar da Maslow'un Temel İhtiyaçlar Hiyerarşisi'nde beşinci ve son sırada bulunan "kendini gerçekleştirme" ihtiyacının birer yan ürünüdür demek yanlış olmaz.

Birey, diğer temel ihtiyaçları karşıladıktan sonra, kendini gerçekleştirme aşamasına gelir. Bu, bireylerin tam olarak potansiyellerini kullanabildikleri bir nokta olarak ta tarif edilebilir. Kendini gerçekleştirme aşamasına geçen bireyler, toplumda söz sahibi olmak isterler ve medyayı bunun bir aracı olarak görürler. Fakat bazı bireyler de medyayı kendini gerçekleştirme aracı olarak gördükleri için, medya da yer almayı kendini gerçekleştirme aşamasına geçişin bir yolu olarak algılarlar. Bunun sonucunda da henüz potansiyel yeteneklerine ulaşmamış, uç örnekler dediğimiz, argo olarak "medya maymunu" diye tabir edilen, olumsuz örnekler de karşımıza çıkabilmektedir. Fakat genel

olarak, gerçekten de toplumun saygı duyduğu, toplumda söz sahibi olan, kendini gerçekleştirmiş bireyler de medya da yer almak isterler. Veya bir diğer açıdan, toplum onların fikirlerini merak eder, medya da görmek ister. Örnek vermek gerekirse, köşe yazarları bunun en iyi örneklerindendir.

1.4.2 Davranışsal İktisat Ve Pazarlama Yöntemleri Açısından Sosyal Medya

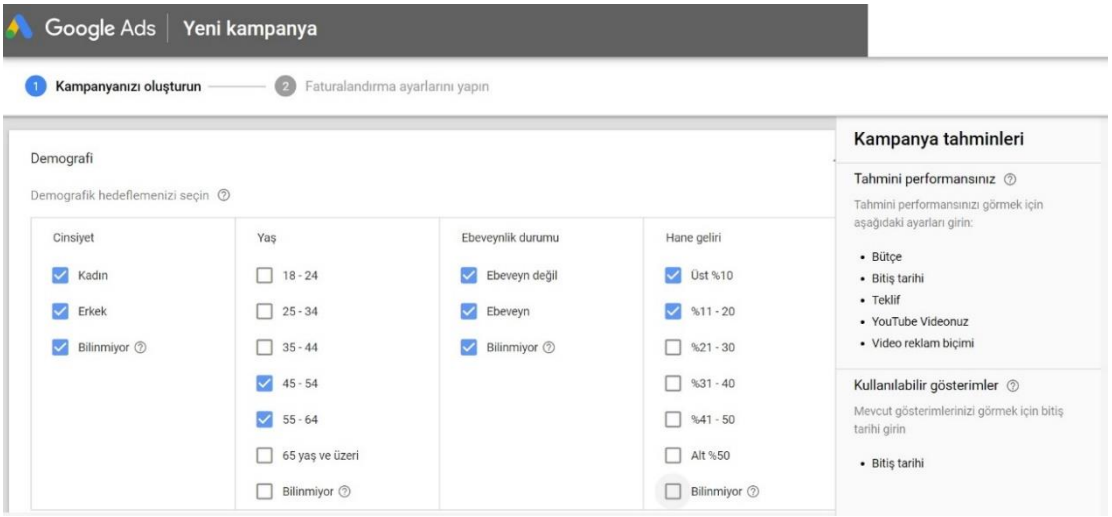
Klasik iktisat teorilerinde bireyler homo economicus, iktisadi akılcı insan veya rasyonel insan olarak tanımlanır. Kısaca, temelleri 1714'te Bernard Mandeville tarafından atılmış olan, sonrasında 1759'da Adam Smith'in Ahlaki Duygular Teorisi'yle katkıda bulunduğu ve 2017'de Richard Thaler'in davranışsal iktisat alanına yaptığı katkılardan dolayı Nobel Ekonomi ödülü almasını sağlayan, davranışsal iktisat ise bu durumun her zaman geçerli olmadığını savunur. Bireyler her zaman tam rasyonel değildir. Sınırlı rasyoneldir ve bazen rasyonel olmayan kararlar verebilmektedirler.

Gene bu konuda 25 yılını FBI'da rehine kurtarma operasyonlarında müzakereci olarak geçirmiş olan Chriss Voss, pazarlama ve ikna teknikleri üzerine yazdığı "Sen Bitti Dediğinde" isimli kitapta, ABD'de FBI'ın rehine kurtarma ve müzakere süreçlerini yeniden tasarlamaya başladıklarında davranışsal iktisat profesörlerinden yardım aldıklarından bahseder. Teorinin odak noktası, insanın her zaman rasyonel olarak hareket etmediği, çoğu zaman duygularıyla hareket ettiğidir. Bu noktada, aslında marjinal fayda kavramına yakın bir durumu ifade eder. Nasıl ki marjinal fayda da tüketilen birimin faydası bireylerin tüketebileceği son birim ile ilgiliyse, yani bireyin o anki doygunluk noktası ile ilgiliyse, davranışsal iktisatta da, bir pazarlama kampanyası, bireylerin duygularını etkileyebildiği kadar, duygularına hitap edip onları ikna edebildiği kadar başarılıdır. Örnek vermek gerekirse; çoğu hazır yemek firması, reklam tabelalarında kırmızı rengi mutlaka kullanırlar ve bunu bilinçli olarak, müşteriler tarafından tercih edilmek için yaparlar. Bu insanların psikolojik yapısıyla ilgilidir. Veya başka bir örnek olarak, sosyal medya platformları amblemlerinde mavi rengi belirli bir oranda kullanırlar ve amblemlerini oval olarak tasarlarlar. Bütün bunlar insan psikolojisine hitap eden, temelde psikolojinin konusu olabilecek tekniklerdir. Fakat bu tür teknikler ve daha pek çok pazarlama tekniği müşteriler tarafından tercih edilme stratejisi olarak kullanıldıklarında, ortaya davranışsal iktisat çıkıyor.

Sosyal medya da gerek erişim oranları açısından, gerekse mütemadiyen insanların her hareketini izleyebilme açısından, davranışsal iktisadın en önemli laboratuvarıdır. Sosyal medya mecraları ve Google tarafından, hareketleriniz kayıt altına alınır. Daha sonra dev veri merkezlerinde bütün bu bilgiler işlenerek, herkesin bir profili çıkartılır. Sonrasında Google ve Facebook, profilinize en çok uyan reklamları size gösterirler. Örneğin çok yorulduğunuzdan veya çok çalıştığınızdan bahseden bir paylaşım yapmışsanız, size tatil reklamı gösterirler. Veya belki paylaşım bile yapmamışsınızdır telefonunuzun GPS'i açıksa ve bir alışveriş merkezinin yakınından geçiyorsanız, telefonunuza orada bulunan ve kampanya yapan firmalardan mesaj gelir.

Aslında belki de bunlara da gerek yoktur. Bir şeyler almaktan veya bir şeye ihtiyacınız olduğundan, telefonunuzun yakınında bahsetmeniz yeterlidir. Telefonunuzun mikrofonu sayesinde bunu analiz edip, reklama dönüştürüp karşınıza çıkarabilirler. Bunun deneyleri dahi yapılmıştır. Bu bir komplo teorisi de değildir. BBC'nin yıllar önce çektiği bir belgeselde sızma testi uzmanları Ken Munro ve David Lodge'yle yapmış oldukları deney bunu doğrulamaktadır. Deneyde standart bir android uygulaması oluşturup google'ın telefon uygulamaları mağazası olan, appstore'a yüklemişlerdir. Sonrasında standart android izinlerini kullanarak, kullanıcıları dinleyip karşılarına onların ilgi alanlarına yönelik reklamlar çıkaracak, bir sistem kurmuşlardır. Bütün bu sistemi kurmaları, iki uzmanın sadece iki günlerini almıştır. Sonuçlar kokutucudur, sistem başarılı bir şekilde çalışmış ve uygulamayı indiren binlerce kişi başarılı bir şekilde dinlenerek davranışlarına yönelik reklamlar karşılarına çıkarılmıştır (https://www.bbc.com/turkce/haberler/2016/03/160302_casus_akilli_telefon, 1.07.2019).

> *İnternet şirketlerinin size dair topladığı veriler arasında, sadece sizin sosyal ağlardaki aktiviteleriniz ile sızdırdıklarınız değil, arkadaş ve aile üyelerinizin sizinle ilgili sızdırdığı veriler de yer alıyor. Bir iş arkadaşınız Google Contacts'e veya iPhone'a adınız ile adresinizi yazdığı anda, Google ile Apple'a kişisel bilgilerinizi de vermiş oluyor. Yeğeninizin, sevgilinizin veya iş ortağınızın doğum gününü Microsoft Outlook takvimine kaydettiğiniz anda, Microsoft da o kişinin doğum gününü öğrenmiş oluyor* (Goodman, 2016, s. 82) peki bunca veri ekonomi açısından ne ifade ediyor?



Şekil 2: Google Adwords
Kaynak: Google reklam verme platformu (https://ads.google.com/aw/campaigns/new, 1.07.2019).

*Google'ın reklam verme platformundan bir görüntü.

Yukarıdaki şekilde google'ın reklam verme platformu olan adwords'ten bir görüntü görülmektedir. Görmüş olduğunuz kısım sadece verilen reklamla ilgili demografik özelliklerin ayarlandığı kısımdır. Bunun dışında hedef müşterinin bulunduğu ülke, bulunduğu il, ilçe, mahalle, ilgi alanları, internete eriştiği cihaz, konuştuğu dil, bize olan uzaklığı, reklamın gösterileceği saatler, günler veya özel bir zaman aralığı, vs. gibi daha yığınla müşteri hedeflemesi filtresi bulunmaktadır. Özetle hedef müşterilerin adı soyadı hariç bütün özellikleri belirlenebilmektedir.

Sistem nasıl işliyor? Örneğin biz ortaçağ barok mimarisine hitap edecek biblolar tablolar veya dekorlar satan, özel üretim yapan bir firmayız diyelim. Bu durumda hedef kitlemizi yukarıda görmüş olduğunuz demografik özelliklerden 20 yaş üstü, üst gelir düzeyine sahip %10'luk dilimden seçip diğer hedefleme ayarlarından ürünle ilgili etiket olarak ortaçağ, barok gibi etiketler koyup, reklamı yayınladığımızda. Sistem örnek veriyorum; ortaçağda geçen bir dizi veya filmi internet üzerinden izleyen, takip eden ve bizim verdiğimiz demografik özelliklere uyan, kişilere bu reklamı gösterecektir. Ortaçağla ilgili kitaplar okuyan, barok mimarisi hakkında herhangi bir ürün aramış veya daha önce almış, herhangi bir şekilde barok mimarisine ilgisi olan, bütün potansiyel müşterilerimize göstermektedir. Buna benzer facebook'un da reklam verme platformları vardır ve aynı şekilde kişilerin ilgi alanları, davranışları, demografik özellikleri, reklamın ne tür içeriklerde gösterileceği, hatta ve hatta farklı farklı reklam içerikleri hazırlayıp

hedef kitleye bunları belirli zaman aralıklarıyla gösterme gibi pek çok seçenek sunulmaktadır.

Sosyal medya reklamcılığı veya dijital pazarlama pek çok açıdan geleneksel medya reklamcılığından ayrılmaktadır. Geleneksel medya da reklamın hedef kitlesi, ilgi alanlarına göre veya demografik özelliklerine göre seçilemez. Fakat sosyal medya ve gelişen teknolojide yukarıda anlattığımız üzere bu mümkündür. Hedef müşterilerin kişisel özelliklerine hitap edebilecek reklam kampanyaları yapmanın, klasik iktisat ile açıklanması zor olacaktır. Fakat konunun başından itibaren belirttiğimiz üzere tam olarak davranışsal iktisadın teorileri ile örtüşmektedir. Bu tür pazarlama stratejilerinde amaç, makul teklif değil kişileri etkileyecek teklif veya kişiye özel, kişiye hitap eden teklif stratejisidir.

1.4.3 Toplum Mühendisliği Ve Sosyal Medya

Şimdiye kadar sosyal medyanın insani ihtiyaçlar açısından veya ekonomik açıdan ne anlama geldiği anlatılmaya çalışıldı. Sosyal medyada bireylerin paylaşım yapma amaçları yada bu mecralarda yer alma, beğenilme gibi isteklerin temel nedenleri iktisat literatüründe yer alan ve bu olgularla bağdaşan teoriler üzerinden tartışıldı. Elbette bu davranışların temel nedenleri aslen psikoloji biliminin bir konusu olacaktır. Burada yalnızca iktisadi açıdan, iktisat ve psikoloji bilimini yakınlaştıran davranışsal iktsiat teorileri üzerinden tartışılmıştır. Fakat sosyal medya da, geleneksel medyanın içinde bulunduğu durum gibi, sadece bireylere veya işletmelere hitap etmemektedir. Bir de bu toplumsal olgunun devlet veya devletler boyutu bulunmaktadır.

"Hükümetin (ABD) interneti (istihbarat için) gözlem altına alması Facebook ve Google'ın buna yardımcı olması ile demokrasi büyük darbe aldı" Julian Paul Assange(2012)'a atfen (Kurtoğlu, 2017, s: 141). Medya ve sosyal medya arasındaki en önemli farklardan birisi geleneksel medya'da bir bireyin paylaşım yapması hayli zordur. Fakat sosyal medya'da herhangi bir şeyi paylaşmak oldukça basit ve ücretsizdir. İkinci en önemli fark ise geleneksel medya çoğu zaman ülkemizde RTÜK(Radyo Televizyon Üst Kurulu) tarafından olduğu gibi, devlet kurumları tarafından denetlenmektedir. Sosyal medyada ise böyle bir denetim mekanizması yoktur. Bu tür denetim mekanizmalarının

eksikliğinden kaynaklı olarak, sosyal medya çoğu zaman bilgi dezenformasyonu, veya bir diğer adıyla bilgi kirliliği olaylarına sıkça sahne olmaktadır.

Toplumlar, çeşitli hassassiyetleri üzerinden, sosyal medyada paylaşılan asılsız veya çarpıtılmış bilgilerle yönlendirilmektedirler. Tabi ki bu tür paylaşımlar rastgele yapılmamaktadır. Kanıtlanması pek mümkün olmamakla beraber, sosyal medya kaynaklı birçok toplumsal olayın arkasında, farklı ülkelerden yönlendirmeler olduğunun izleri görülmektedir. Toplumun tercihlerini ve algısını değiştirme yönünde operasyonlar yapılabildiğinin en güzel kanıtlarından birisi, Amerikan Davranış Araştırmaları ve Teknolojisi Enstitüsü'nden psikolog Dr. Robert Epstein'in yaptığı araştırma sonucunda, google'ın arama motoru maniplasyonu ile dünyadaki seçimlerin %25 ini etkilediğini belirtmesidir. Ve ABD seçimlerinde Google'ın Hillary Clinton lehine arama sonuçları çıkardığı iddia edilmiştir. Bunlar dışında ülkemizde de, sosyal medyada bir takım uygunsuz görüntüleri veya haklarında yayınlanan asılsız iddialar yüzünden, siyasi hayatları biten bir çok politikacı mevcuttur.

Bunlara ek olarak, gene benzer mantıkla hazırlanan, viral reklam denilen olgu bulunmaktadır. Bu da belirli bir düzeyde toplum mühendisliği gerektiren, bir çeşit reklam stratejisidir. Bu tarz toplumun beğenisine hitap eden reklamlar bir çığ gibi sosyal medyada yayılmaktadır. Reklam olsun, karalama kampanyaları olsun veya siyaseti dizayn etme amaçlı paylaşımlar olsun bütün bu bahsedilen durumların elbette ekonomik etkileri de bulunmaktadır. Fakat bunu ölçümlemek günümüz imkanlarıyla şuan için mümkün değildir. Sözel olarak betimlemek gerekirse bir firmanın viral bir reklam tuttundurmayı başarması, bütün tv kanallarına reklam vermesinden çok daha fazla etkiye sahiptir. Ekonomik olarak geri dönüşü büyüktür.

Küçük bir örnek vermek gerekirse, bir zamanlar meşhur olan stres çarkı buna en güzel örneklerden biridir. Kimse tv de stres çarkının reklamını yapmamıştır. Tamamen sosyal medyada meşhur olduğu için milyonlarca satmıştır. Siyasi açıdan ise milyonlarca lira harcanarak oluşturulan bir siyasi kimliğin, sosyal medyada yıkılması, söz konusu siyasiye ve siyasi partiye milyonlarca lira zarara yol açmaktadır. Fakat zararın tamamı bu değildir. Söz konusu ülke açısından, siyasetin bu şekilde dizayn ediliyor olması, ölçümlenemeyecek derece büyük toplumsal ekonomik zararlar doğuracaktır. Ekonomide bu olgu, bir noktada kredibilite ile bağlantılıdır. Örnek vermek gerekirse, herhangi bir

ülkenin ekonomi karar vericileri hakkında çıkan en ufak bir olumsuz haberin etkisi, borsada kayıplar olarak dönmektedir.

1.4.4 Siber Savaş Alanı Olarak Sosyal Medya

Google yöneticisi Wael Ghonim, 2010 yılında Arap Baharı'nda bir facebook sayfası açıp, Hüsnü Mübarek'in özel güvenlik kuvvetlerinin genç bir Mısırlı protestocuyu öldürme görüntülerini yayınlamıştı. Görüntüler yayınlandıktan iki dakika sonra sayfaya 300 kişi katıldı. Üç ay içinde ise katılım 250.000'i geçti (Goodman, 2016, s. 72). Goodman'ın aktardığı örnekte görüldüğü gibi, sosyal medya da bir kontrol mekanizması olmadığı için, bu tür toplumda infial oluşturacak veya toplumun hassasiyetlerine hitap eden paylaşımlar, çığ gibi büyümekte ve yayılmaktadır. Elbette son zamanlarda sosyal medya mecraları, şikâyet edilen paylaşımları kaldırmak gibi bazı önlemler almışlardır. Fakat bu tür paylaşımları engellemek neredeyse imkânsızdır. Bir kişi yükleyip paylaştıktan sonra, zincirleme olarak etkileşime girerek oradan oraya yayılır.

Sosyal medya siber savaş alanı olarak birçok farklı yolla kullanılabilir:

1) İstihbarat toplamak için sosyal medya kullanımı
2) Siyaseti dizayn etme amaçlı olarak sosyal medya kullanımı
3) Bilgi kirliği ve karalama kampanyaları ile ülkelerin itibarına yönelik suikastlar
4) Ekonomik spekülasyon amaçlı yalan haberler yaymak amacıyla kullanımı
5) Hacking yöntemi olarak kullanımı

Mete Han'ın M.Ö. 209'da ilk düzenli orduyu kurmasından bu yana, ordular stratejik ve planlı hareket ederler ve savaş planları yaparlar. Bu doğrultuda Sun-Tzu'nun savaş sanatı eserinde de sıkça geçen, ve artık günümüzde standart haline gelmiş bir takım taktikler vardır. Savaşı başlatmadan önce düşman hakkında öğrenilebilecek her şeyi öğrenmek, mümkünse aralarına istihbarat subayları göndermek, savaşılacak ülkenin halkının desteğini almanın yollarını aramak(bu genelde mevcut yönetimi ve yöneticileri kötüleyici haberler yayarak olur), düşman ordusu içerisinde kendinize çekebileceğiniz askerler aramak ve daha fazlası.

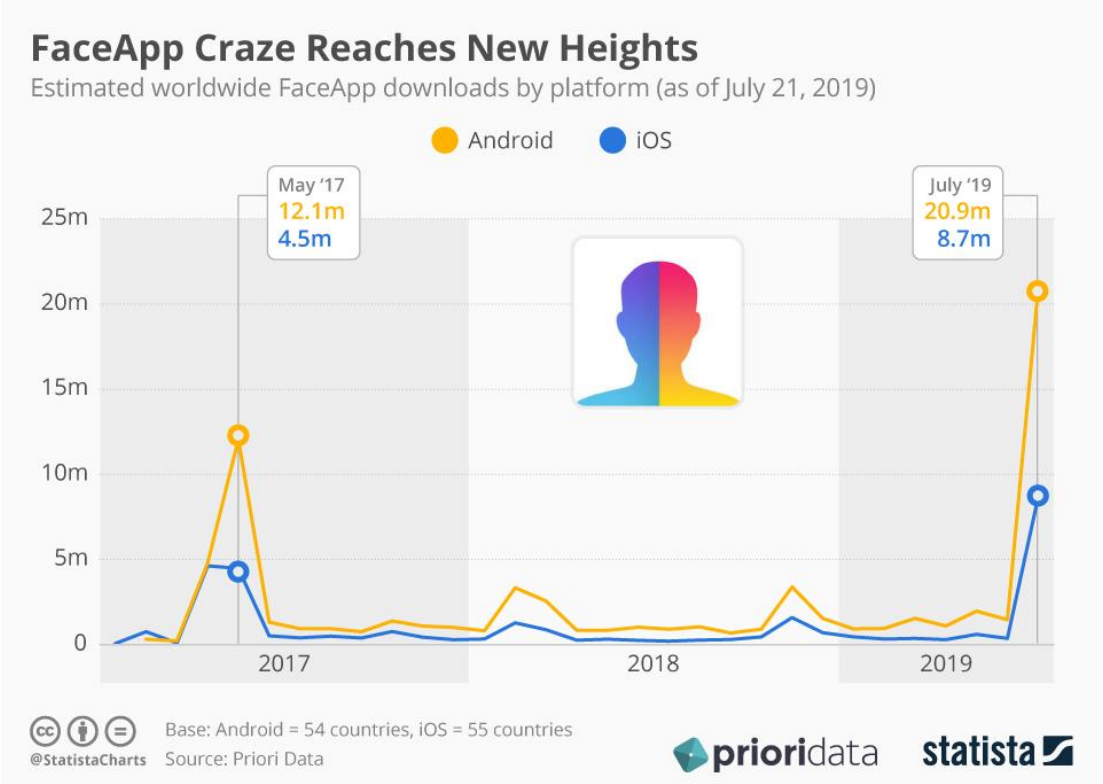
Bu taktiklerin uygulanması eski devirlerde uzun zaman alan bir hazırlık ve ciddi çabalar gerektirmekteydi. Fakat günümüzün beşinci savaş alanı olarak tanımlanan siber

âlemde, bu savaş taktiklerini uygulamak neredeyse masrafsız ve eskisine göre neredeyse hiç zahmete girmeden oldukça yüksek başarıyla sonuçlanmaktadır.

1) İstihbarat toplamak amacıyla sosyal medya'nın kullanımı:

Daha önceki alt başlıklarda bahsedildiği gibi, sosyal medya da insanlar paylaşımları bir takım insani ihtiyaçlardan dolayı gönüllü olarak yaparlar. Sosyal medya veya sosyal medya uygulamaları, istihbarat servisleri için deyim yerindeyse altın yumurtlayan tavuktur. Milyarlarca insan kendisi arkadaşları, çevresi ve yaptığı şeyler hakkında sürekli veriler yükler. Yüklenen bu veriler, büyük veri işleme merkezlerinde işlenir, tasniflenir ve istihbarata dönüştürülür. Çoğu devlet, terör örgütleri ve hackerlar bu ücretsiz istihbarat toplama kaynaklarını etkin bir şekilde kullanırlar. Bu konuyla ilgili güncel bir örnek vermek gerekirse, insanların güncel fotoğrafları üzerinden yaşlı hallerini gösteren "FaceApp" isminde bir yaşlandırma uygulaması, 2017 yılında 95 farklı ülkede en çok kullanılan uygulama olmayı başarmıştır. Uygulamanın yapımcısı ise Rusya, Saint Petersburg'da bulunan Wireless Lab şirketidir. Şirketin yöneticisi Yaroslov Goncharov ise daha önce Yandex'in mobil platformunun liderliğini yapmıştır ve Petersburg Devlet Üniversitesi'nden bilgisayar bilimleri üzerine mastır derecesi bulunmaktadır. (https://www.haberturk.com/faceapp-yaslandirma-uygulamasinin-arkasinda-ne-var-2504946-teknoloji, 17.07.2019).

Bu verilerin, Rus İstihbaratı KGB'nin eline geçmeyeceğine dair kimse garanti veremez. Bir diğer çarpıcı örnek te Facebook firmasının kullanıcılarının onayını almadan elde ettiği verileri, Cambridge Analytica adlı veri analiz şirketine satması olayıdır.



Grafik 5: FaceApp Kullanımı

Kaynak: Statista, (https://www.statista.com/chart/18769/estimated-worldwide-faceapp-downloads-by-platform/ , 21.07.2019)

Grafik 5'te android ve İOS(Iphone Operation System) kullanıcılarının, FaceApp uygulamasını indirme sayıları gözükmektedir. Uygulama yaklaşık 21 milyon android kullanıcısı ve yaklaşık 9 milyon IOS kullanıcı olmak üzere, toplamda 30 milyona yakın kullanıcı tarafından indirilmiştir. Grafikte görülen uygulamanın indirme trendidir. İndirip telefonunda muhafaza eden veya silenlerin sayısı bilinmemektedir. İlaveten uygulamayı indiren 30 milyon kişinin sadece kendi resimleri üzerinde kullanmayıp arkadaşı, ailesi ve çevresindeki insanların resimleri üzerinde de kullandığı göz önüne alındığında, uygulamanın hatırı sayılır sayıda insanın resimlerine ve dosyalarına ulaştığını söylemek mümkündür.

Siyaseti dizayn etme amaçlı sosyal medya kullanımı:

Bazı durumlarda bir ülkeyi işgal etmek, ya da doğrudan savaş açmak yerine, içeriden müttefikler bulup, düşmanın kaynaklarını kendi lehinize kullanmak, daha yararlı olabilir. Mete Han'ın, Çin'i vergiye bağlayıp, orayı işgal etmeden bırakması, bunun bir örneğidir. Günümüzdeki örnekleri bakımından, Türk Savaş Tarihi'ni iyi derecede

araştıran, ABD'nin Irak'ta uyguladığı taktik de bunun aynısıdır. Irak'ın kaynaklarını kullanmak için savaşmış ve amacına ulaşmıştır. Fakat orada sadece bu kaynakların akışının güvenliğini sağlama amaçlı tedbirler almıştır. Irak'a yerleşmemiştir. Bunun günümüzdeki en güzel örneği ise CIA'in Venezuela'ya yapmaya çalıştığı darbe operasyonlarıdır. CIA, Hügo Chavez hükümetinin başa geçmesiyle Venezuela'dan kovulan ABD petrol şirketlerini, yeniden Venezuela'da faaliyete geçirebilmek için, sosyal medya ve medya yoluyla muhalefeti ve destekçilerini Chavez'e karşı kışkırtmış ve darbe yapmaya kalkışmıştır, fakat başarılı olamamıştır. CIA'in bu girişimleri günümüzde Venezuela'nın mevcut lideri Nicolas Maduro üzerinde halen devam etmektedir. Maduro karşıtları sosyal medya üzerinden örgütlenerek sokaklara dökülmüştür fakat darbe girişimleri gene başarısız olmuştur.

3)Bilgi kirliği ve karalama kampanyaları ile ülkelerin itibarına yönelik suikastlar:

Bilgi dezenformasyonu veya bilgi kirliliği olarak tanımlanan olgu da gene ülkelerin birbirlerine karşı veya duruma göre kendi halklarına karşı, çeşitli sebeplerle etkin olarak kullandıkları bir savaş taktiğidir. Tarihten örnek vermek gerekirse Hitler Almanyası'nda halk devletin yaptığı yanıltıcı radyo yayınları yüzünden, Rus Ordusu Berlin'e varana dek savaşı kazandıklarını düşünüyordu. Veya güncel örnek olarak her iki kapsama da girebilecek Kuzey Kore örneği bulunmaktadır. Kuzey Kore'deki halkın dış dünyadan tamamen kopuk yanlış haberlerle idare edildiği söylenmektedir. Bu bilgi eğer doğruysa Kuzey Kore Devleti'nin kendi halkına uyguladığı bir bilgi kirliliği örneğidir. Şayet bu bilgi doğru değilse bu bilgiyi sosyal medyada ve medya da yayan taraf ülkeler, Kuzey Kore Hükümeti'ne karşı bilgi kirliliği yoluyla karalama kampanyası yürütmektedirler. Ülkemiz açısından da Milli İstihbarat Teşkilatı (MİT)'nın tırlarla, Irak-Şam İslam Devleti isimli terör örgütü (DEAŞ)'e silah taşıdığı söylentileri de, gene bir takım dış devletlerin ülkemize yapmaya çalıştığı bir tür bilgi kirliliği yoluyla karalama kampanyası örneğidir. Bu asılsız iddiaların sosyal mecralarda dolaşmasından dolayı ülkemiz uluslararası siyasi arena da ciddi anlamda sıkıntıya girmiş ve ekonomik açıdan da zarara uğramıştır.

4) Ekonomik spekülasyon amaçlı yalan haberler yaymak amacıyla kullanımı:

Ekonomik spekülasyon amacıyla sosyal medyanın kullanımına örnek olarak, saldırı örnekleri kısmında Suriye Elektronik Ordusu (SEA)'nın 23 Nisan 2013'te Associated Press Haber Ajansı'nın Twitter hesabını hackleyerek, Obama yaralandı diye asılsız haberler yaymaları sonucu, Dow Jones endeksinde 140 puanlık bir düşüşe neden olması örnek gösterilebilir. Bunun gibi pek çok asılsız haber furyası stratejik olarak hazırlanıp, ekonomik çıkarlar elde etme amacıyla hedefe yönelik kullanılabilmektedir. Bu tür operasyonlarda ülkelerin başkanları, dev şirketlerin yöneticileri veya devletlerin ekonomi bakanları hedef alınabilir. Amaca yönelik olarak hedef belirlenir.

5) Hacking yöntemi olarak kullanımı:

Saldırı araçları kısmında anlattığımız, oltalama(Phishing) yöntemi ile hedeflerin sosyal medya hesapları ele geçirilerek, hedeflerin bizzat kendilerinden veya yakınlarından, para isteme veya şantaj amaçlı olarak, özel yazışma ve resimlerini kullanma yöntemidir. Bu durumun ülkemizde yaşanmış pek çok örneği mevcuttur. Bu yöntemin etkili bir şekilde kullanımı için, bir diğer hacking yöntemi olan sosyal mühendislik yani karşısındaki kişiyi inandırma becerisi de gerekebilmektedir. Bu durumun en iyi örneklerinden birisi, geçtiğimiz yıllarda magazin dünyasının ünlülerinin başına gelmiştir. Milliyet gazetesinin haberleştirdiği olay aşağıda anlatıldığı gibi gerçekleşmiştir.

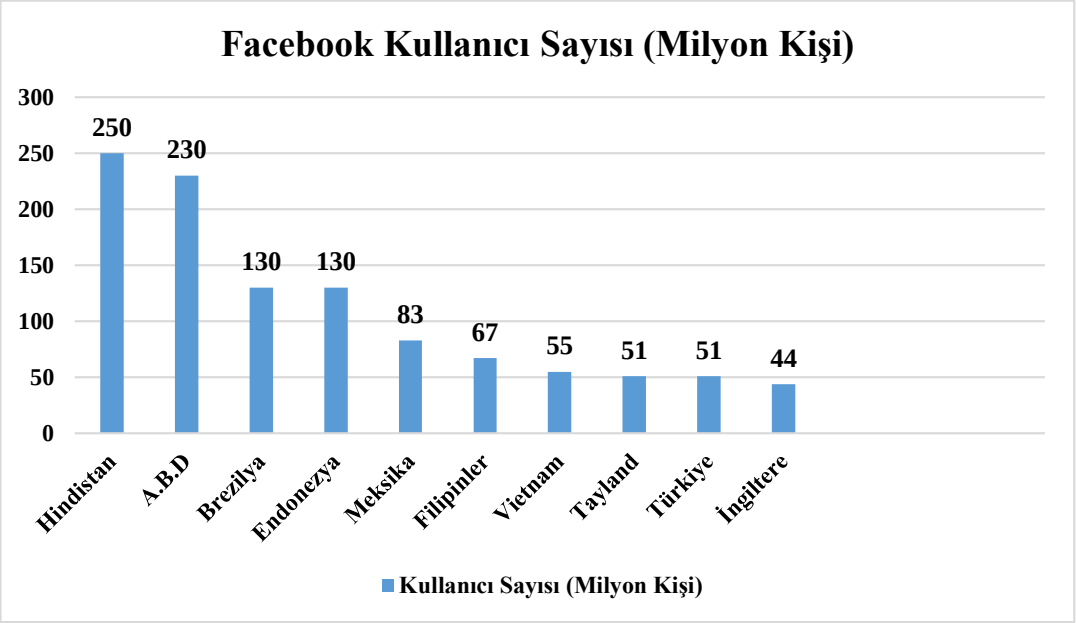
> *Fishing(olta) yöntemi ile ünlü kişilerin sosyal medya hesaplarını çalarak rüşvet karşılığında geri vermeyi teklif eden Ducky Layne çetesi sonunda yakalandı. Tamer Karadağlı, Gamze Özçelik gibi ünlü oyuncuların yanında Orkun Işıtmak, Enes Batur, Berkcan Güven gibi son derece ünlü sosyal medya ünlülerin hesabı çalınmış ve bu hesapların hakkında kısmına "Ducky.Official" yazılmıştı.*
>
> *Başlarını Gökyar Ş'nin çektiği çetede, 42 şüpheli gözaltına alındı ve bunların 14 tanesi siber suçlardan dolayı tutuklandı. Aleyna Tilki'ye olan benzerliğini kullanan çete üyesi Bahar Ç.'nin (22) sahte kimlikle, Facebook'a 'sahte hesap' şikâyetinde bulunduğu ve şarkıcının hesabını kapattırdığı öğrenildi. Çete üyesi olduğu iddia edilen Bahar Ç.'nin 500 bin civarında sosyal medya takipçisiyle sosyal medyanın fenomen isimlerinden olduğu öğrenildi. Çetenin ünlü ismi Nusret'in de hesabına girdiği, ancak polis operasyonu nedeniyle hesabı ele geçiremedikleri öğrenildi. Tarık Mengüç, Erdal Özyağcılar, Tamer Karadağlı gibi ünlü isimlerin de yer aldığı 6000'den fazla sosyal medya hesabı ve WhatsApp konuşmalarını ele geçiren suç örgütü üyelerinin ne ceza*

alacakları şu an için bilinmiyor (http://www.milliyet.com.tr/teknoloji/unlulerin-sosyal-medya-hesaplarin-calan-turk-cetesi-yakalandi-2540797, 1.07.2019).

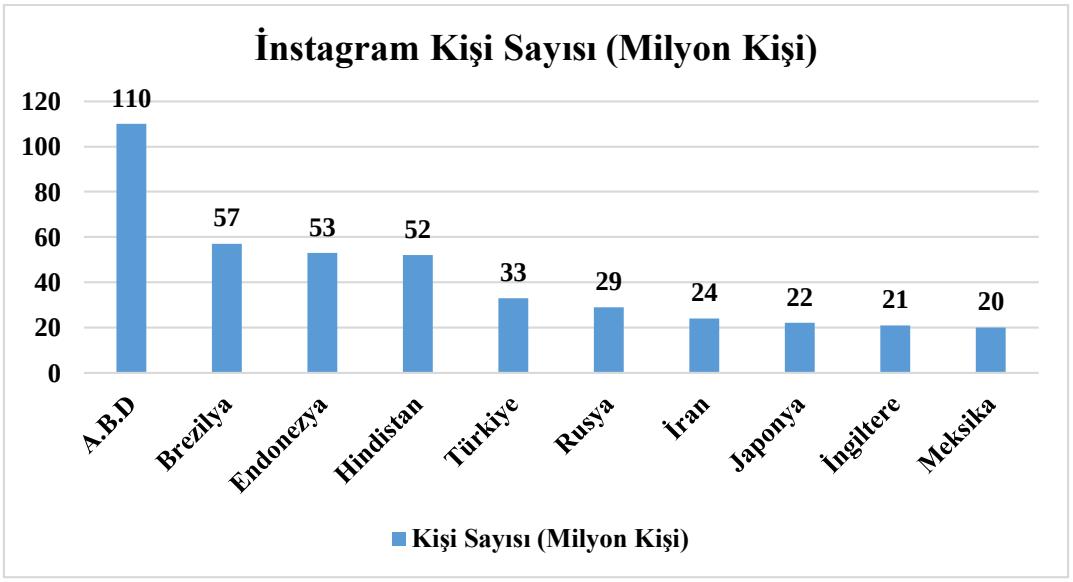
1.4.5 Sosyal Medyada Etkin Hedef Belirleme Stratejisi

Son olarak yukarıda anlattığımız sosyal medya kitlelerini harekete geçirmek için veya kampanyalar yürütmek için de belirli bir strateji dahilinde hareket edilmesi gerekmektedir. Grafik 6 ve 7'de facebook kullanımında ilk on ülke ve İnstagram kullanımında ilk 10 ülke kullanıcı sayıları ile görülmektedir. Dikkat ettiğimizde kullanılan sosyal medya platformuna bağlı olarak ülkelerin kullanıcı sayıları ve dolayısıyla sıralamaları değişmektedir. Bu grafiklerin devamında (Kahraman,2016) kaynağından alınan verilerle tarafımızdan oluşturulan tablo 1'de ise pek çok sosyal medya platformunun paylaşım sayısı, günü ve saatine yönelik bilgiler verilmiştir. Bu bilgilerin nasıl kullanılacağına ilişkin bir örnek vermek gerekirse ABD'yi hedef alan bir sosyal medya çalışmasında Facebook yerine İnstagram platformunda çalışılması gerektiği veriler ışığında açık bir şekilde görülmektedir. Platformu seçtikten sonra ikinci adım olarak tablo 1'de görüldüğü üzere İnstagram platformunda en iyi etkileşim günü pazartesidir. Çalışmanın gününü de belirledikten sonra saat olarak 07:00-18:00 arası gene tablo 1'de görüldüğü üzere İnstagram platformu için en iyi etkileşim saatleridir. Sonrasında da günlük 5-10 arası paylaşımın en ideal paylaşım sayısı olduğu görülmektedir. Bu kurallara uyularak uygulanan bir sosyal medya çalışmasının, veriler ışığında en etkin sosyal medya çalışma olması beklenmektedir.

Veya başka bir bakış açısıyla siber saldırılar sonucunda aksayan internet bağlantısından kaynaklı olarak, sosyal medya kullanılamamasının ekonomik etkisi de sosyal medya platformuna, güne ve saate göre değişmektedir.



Grafik 6: Facebook Kullanıcı Sayısında İlk 10 Ülke
Kaynak: Veri Kaynağı, Digital in 2018 Global Overview



Grafik 7: İnstagram Kullanıcı Sayısında İlk 10 Ülke
Kaynak: Veri Kaynağı, Digital in 2018 Global Overview,

Grafik 6 ve 7'de Facebook ve İnstagram kullanıcı sayıları verilmiştir ve görüldüğü üzere kullanıcı sayıları ülkelere göre farklılık göstermektedir. Tablo1'de ise sosyal medya mecralarının en iyi paylaşım istatistikleri verilmiştir. Bu istatistikler de sosyal medya platformları arasında farklılık göstermektedir. Bu istatistikler göz önüne alındığında her kullanıcının kullanım saati ve yaşadığı coğrafya ya özgü bir sosyal medya algısı ve bu algı üzerinden de hedef kitlesi oluşmaktadır.

Tablo 1: Sosyal Medya Paylaşımlarına Yönelik İstatistiki Bilgiler

PLATFORM	En İyi Günler	En Kötü Günler	En iyi saatler	En Kötü Saatler	İdeal Paylaşım
Facebook	Çarşamba	Cumartesi ve Pazar	13:00-16:00 arası en iyi saat ise 15:00	00:00-08:00 arası	Günde 1-2
Twitter	Pazartesi, Salı, Çarşamba, Perşembe	Cumartesi ve Pazar	13:00-18:00 Arası	00:00-08:00 arası	Günde 4-5
İnstagram	Pazartesi	Pazar	07:00-18:00 arası	00:00-06:00	Günde 5-10
Linkedin	Salı, Çarşamba, Perşembe	Pazartesi, Cuma	07:00-17:00 ile 18:00 arası	22:00-06:00	Haftada 5-7 Günde 1

Kaynak: (Kahraman, 2016, s:42-47)

1.5 YAZILIM (PROGRAM)

Bilgisayarlar uzun seneler ele alınmamış büyüklükler hakkında sayısal ve mantıksal işlemler yapmayı sağlamışlardır. Fakat böyle bir sistemi kullanmak, makineye soru sormak, cevap almak ve komut vermek için makinenin içyapısına göre bir dil kullanmak gerekir (Bakoğlu, 1975:21). Bilgisayarın ilk örnekleri dişli çarklar ve delikli kartlar vasıtasıyla bir takım işlemler yapabilirken, elektroniğin işin içine girmesiyle birlikte delikli kartların yerini 1'ler ve 0'lar açık veya kapalı mantığı almıştır.

Bilgisayarlar, birçok parçadan oluşurlar ve en önemli parçaları, asıl bilgi sayma işlemini yapan parçaları işlemcileridir. Günümüzde çeşitli işlemci mimarileri mevcut olmakla birlikte, hepsinin temel çalışma prensibi aynıdır. Bilgiyi saymak için 1'ler ve 0'lardan oluşan, binary(ikili) sayı sistemi üzerine kurulmuştur. Bu sistem veri biliminin temellerini oluşturmuştur. Binary kelimesinden Binary Digit(sayı, hane, basamak) kelimesinin kısaltması olan, bit terimi türemiştir. Bu 1 ve sıfırlardan her birisi bir bit uzunluğundadır, ya da diğer bir deyişle ikili sayı sisteminde tek haneli bir sayıdır. 1940'lı yıllarda MIT'de uzun süredir yarı iletkenler, transistörler ve veri iletiminin temelleri üzerine çalışan Claude Elwood Shannon, bir mesajın bilgi içeriği ve büyüklüğünü

mühendislerin “bit” olarak tanımladıkları bir birimle hesaplamanın en faydalı yöntem olacağını düşünüyordu. Daha önce hiç kullanılmamış olan bu “bit” kelimesini Shannon, Bell Laboratuvarları’ndan arkadaşı olan, John Tukey’den öğrenmişti (Gertner, 2013:114). Shannon’un teorisinden yıllar sonra 1961 Mayıs’ında Bob Benner, bilgisayar iletişimini daha verimli kullanmak amacıyla standart bir kod sistemi geliştirmek için, Amerikan Ulusal Standartlar Enstitüsü’ne(ANSI) bir teklif gönderdi. Ve günümüzde kullanılan American Standard Code for Information Interchange (ASCII) Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi meydana çıktı.

En basit tabirle bu kodlama sistemi mors alfabesi gibi bir mantıkla çalışır, tek bir farkla uzun kısa yerine 0 ve 1’ler vardır. Daha sonra binary mimarisinin üzerine, 8 bitlik dizilerden oluşan octal, 10’luk sayı sistemine dönüştürmek için decimal, ve 16’lık sayı sistemi olarak kullanılan hexadecimal tabanda kullanımları ortaya çıkmıştır. Her 8 bitlik dizi ASCII tablosunda bir harf veya karaktere denk geldirmektedir.

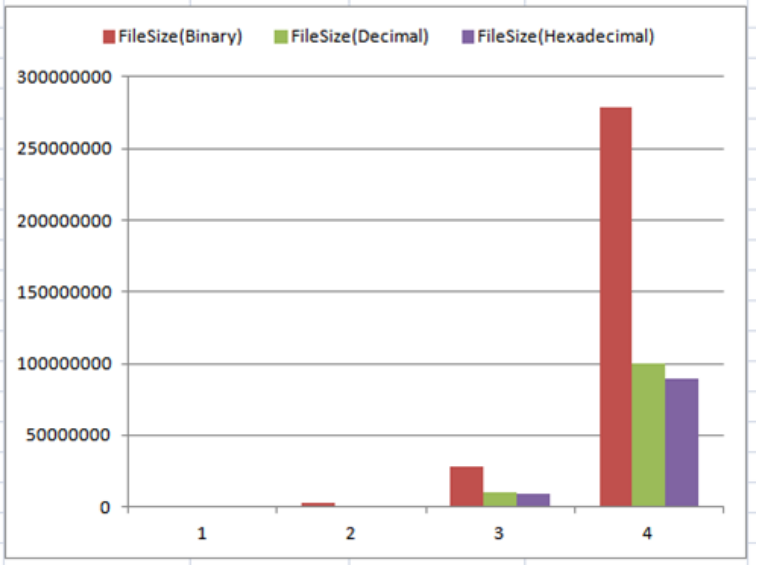
Char	Dec	Oct	Hex	Char	Dec	Oct	Hex	Char	Dec	Oct	Hex
(sp)	32	0040	0x20	@	64	0100	0x40	`	96	0140	0x60
!	33	0041	0x21	A	65	0101	0x41	a	97	0141	0x61
"	34	0042	0x22	B	66	0102	0x42	b	98	0142	0x62
#	35	0043	0x23	C	67	0103	0x43	c	99	0143	0x63
$	36	0044	0x24	D	68	0104	0x44	d	100	0144	0x64
%	37	0045	0x25	E	69	0105	0x45	e	101	0145	0x65
&	38	0046	0x26	F	70	0106	0x46	f	102	0146	0x66
'	39	0047	0x27	G	71	0107	0x47	g	103	0147	0x67
(	40	0050	0x28	H	72	0110	0x48	h	104	0150	0x68
)	41	0051	0x29	I	73	0111	0x49	i	105	0151	0x69
*	42	0052	0x2a	J	74	0112	0x4a	j	106	0152	0x6a
+	43	0053	0x2b	K	75	0113	0x4b	k	107	0153	0x6b
,	44	0054	0x2c	L	76	0114	0x4c	l	108	0154	0x6c
-	45	0055	0x2d	M	77	0115	0x4d	m	109	0155	0x6d
.	46	0056	0x2e	N	78	0116	0x4e	n	110	0156	0x6e
/	47	0057	0x2f	O	79	0117	0x4f	o	111	0157	0x6f
0	48	0060	0x30	P	80	0120	0x50	p	112	0160	0x70
1	49	0061	0x31	Q	81	0121	0x51	q	113	0161	0x71
2	50	0062	0x32	R	82	0122	0x52	r	114	0162	0x72
3	51	0063	0x33	S	83	0123	0x53	s	115	0163	0x73
4	52	0064	0x34	T	84	0124	0x54	t	116	0164	0x74
5	53	0065	0x35	U	85	0125	0x55	u	117	0165	0x75
6	54	0066	0x36	V	86	0126	0x56	v	118	0166	0x76
7	55	0067	0x37	W	87	0127	0x57	w	119	0167	0x77
8	56	0070	0x38	X	88	0130	0x58	x	120	0170	0x78
9	57	0071	0x39	Y	89	0131	0x59	y	121	0171	0x79
:	58	0072	0x3a	Z	90	0132	0x5a	z	122	0172	0x7a
;	59	0073	0x3b	[	91	0133	0x5b	{	123	0173	0x7b
<	60	0074	0x3c	\	92	0134	0x5c	|	124	0174	0x7c
=	61	0075	0x3d	]	93	0135	0x5d	}	125	0175	0x7d
>	62	0076	0x3e	^	94	0136	0x5e	~	126	0176	0x7e
?	63	0077	0x3f	_	95	0137	0x5f				

Şekil 3 : Binary Table
Kaynak: IBM

(*https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ioaq100/ascii_table_appendix.htm 6.7.2019)*

Sistem şekil 3'de örnek bir ASCII tablosunda, görüldüğü gibi işlemektedir. Binary den sonraki sistemlerin inşa edilme sebebi ise daha çok verinin, daha az yer ayırarak saklanmak istenmesidir. Fakat bu durumda bilgisayar veriyi işleme sokmak için tekrar binary haline geri çevirmek zorunda olduğundan, işlem hızı düşmektedir. Dosya sıkıştırma uygulamalarından aşina olduğumuz üzere, veri ne kadar çok sıkıştırılırsa, sıkıştırılmış dosyayı tekrar eski haline getirmek veya işleme sokmak, o kadar uzun süre almaktadır. Aşağıdaki grafikler incelendiğinde bu tezat daha iyi anlaşılacaktır.

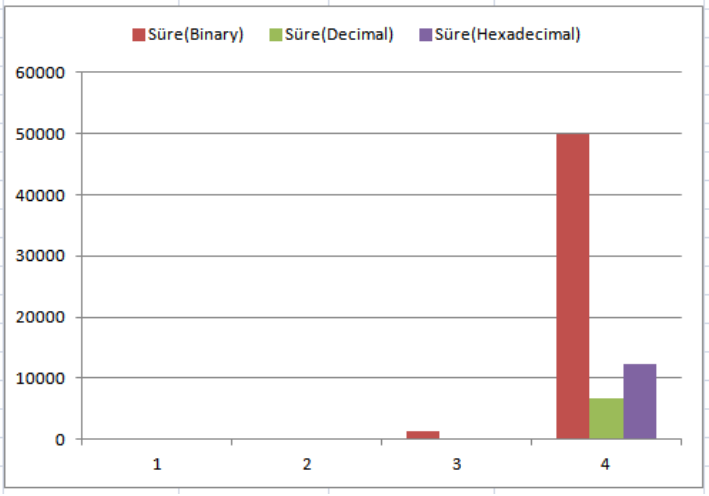
Deneme Uzunluğu	FileSize(Binary)	FileSize(Decimal)	FileSize(Hexadecimal)
1000	278959	100000	89103
10000	2790570	1000000	891512
100000	27907295	10000000	8915506
1000000	279069235	100000000	89152065



Grafik 8: Binary Hex Octal Farkı
Kaynak:https://www.buraksenyurt.com/post/Decimal-to-Binary-to-Hexadecimal 6.7.2019

Grafik 8'de görüldüğü üzere kırmızı renkle temsil edilen binary düzende saklanan verilerin boyutu en yüksek iken mor ile temsil edilen hexadecimal verilerin boyutu en düşüktür.

Deneme Uzunluğu	Süre(Binary)	Süre(Decimal)	Süre(Hexadecimal)
1000	107	143	37
10000	50	21	23
100000	1328	156	161
1000000	49971	6669	12216



Grafik 9: Binaryı Hex Octal Farkı 2
Kaynak:https://www.buraksenyurt.com/post/Decimal-to-Binary-to-Hexadecimal 6.7.2019

Grafik 9'da ise az önceki durumun tersine işlem süresi binary düzende daha uzun iken decimal düzende en kısadır.

Bilgisayarlarda bulunan işlemci mimarileri de bu yapılara göre isimlendirilmektedir. 32 bit ve 64 bit işlemci mimarisi arasındaki fark, birisi her döngüde 32 bit uzunluğunda veri işlerken diğeri 64 bit uzunluğunda veri işlemektedir. Verimli kullanım açısından programcılar da bu farkları dikkate alarak programlar yazmaktadırlar. Bu yüzden 64 bit mimariye sahip bir bilgisayar, 32 bit işletim sistemleri ve programlarını çalıştırabilirken tersi mümkün değildir. Çünkü işlemciye gönderilen 64 bitlik dizinin 32 bitten sonrasını 32 bitlik işlemciler anlamlandıramamaktadırlar.

Bütün bu tablolar veri yapıları gibi argümanların kullanımının yol açtığı karmaşadan ve zorluğundan kurtulmak için derleyiciler ve programlama dilleri geliştirilmiştir. Programlama dilleri düşük seviye diller, yani makine diline en yakın olan dillerdir, sonra orta seviye ve insan diline yaklaştıkça yüksek ve çok yüksek seviye diller olarak adlandırılmaktadır. Derleyiciler ise kısaca yazılan kodları bir programlama dilinden daha düşük seviyedeki başka bir programlama diline çeviren programlardır. Yani bilgisayarlarda daha kolay işlem yapmak amacıyla programlama sistemleri veya diğer bir deyişle programlama dilleri geliştirilmiştir.

Programlama dillerinin gelişimi ile birlikte Operation System (OS), işletim sistemleri geliştirilmeye başlanmıştır. Örneğin bugün hala Windows işletim sistemlerinde mevcut bulunan Microsoft Disk Operating System (MS-DOS) Microsoft'un geliştirdiği ilk işletim sistemidir. Nereden nereye geldiğimizi anlamak için iyi bir örnektir. Sonrasında pencere sistemi ve kullanıcı ara yüzleri geliştirilmiş ve günümüzde kullanmakta olduğumuz programlar ve işletim sistemleri halini almıştır.

1.6 ALGORİTMA

Belirli bir problemi çözmeye yönelik kurulmuş formül veya bilgisayar bilimi açısından program kışı olarak açıklanabilir. Programlama yapılırken öncelikle problemin çözümüne yönelik veya uygulamaların kullanımına yönelik bir akış şeması oluşturulur sonrasında ise bu şemaya uygun olarak programın yazımı gerçekleştirilir.

Aşağıda ucuza sağlıklı beslenme amacıyla İstanbul İşletme Enstitüsü'nün programlama dersinde yazmış olduğum bir algoritma örneği görülmektedir:

1-Başla

2-//1. Modül

3-// Açlık Durumu Kontrolü

4-Akıllı saat ile iletişime geç

5-Kişinin açlık durumunu kontrol et

6-Akıllı saatten gerçek zamanı öğren

7-Hangi zaman diliminde olduğunu tespit et (sabah, öğlen, akşam, ara öğün)

8-Gerçek zaman ve ideal yemek yeme zamanı arsındaki farkı hesapla

9-İdeal yemek yeme zamanına kalan süre [<=fark] ise 2. Modüle geç değilse başa dön

10-//2. Modül

11-//Yemek Tarifi Seçimi

12-Akıllı saate bağlan kişinin kalori ihtiyacını öğren

13-Yemek tarifleri veri tabanına bağlan ve kişinin kalori ihtiyacına en yakın olan 5 yemek tarifini belirle

14-Mutfağa bağlan ve bu 5 tarif arasından gerekli malzemelerin mevcut olanlarını belirle.

15-Bu 5 tarif arasından gerekli malzemelerin mutfakta mevcut ve son kullanma tarihi en yakın olanları belirle.

16-Mevcut malzemeler ve son kullanma tarihleri kriterlerini en çok karşılayan yemek tarifini belirle.

17-İnternete bağlan zincir marketlerin çevrimiçi mağazalarından tarifler için gerekli malzemelerin tutarını hesapla.

18-Her tarifin maliyetini ayrı ayrı hesapla

19-Yemek tariflerini en düşük maliyetli olandan en yüksek olana göre sırala.

20-Akıllı saat ile iletişime geç

21-Kişiyi yemek saati yaklaştığına dair uyar

22-Kişi ertele butonuna basarsa uyarıyı 10 dk. ertele

Kişi menüleri gör butonuna basarsa maliyet ve mevcut malzeme butonlarını göster.

23-Kişi maliyet butonuna basarsa maliyetine göre sıralanan listeden yemek adları ve yanında eksik malzeme sayılarını yaz.

24-Kişi mevcut malzeme butonuna basarsa yemek tariflerini mevcut malzeme sırasına göre göster.

25-Akıllı saate bağlan kişinin konum bilgisini öğren.

26-İnternete bağlan ve konum bilgisine en yakın ve en düşük maliyetli marketlerin konumunu öğren.

27-Akıllı saate bağlan ve kişiye tespit edilen marketin konumunu ve eksik malzeme listesi butonunu göster.

28-Kişi eksik malzemeler butonuna basarsa eksik malzemelerin listesini ve hedef marketteki fiyatlarını ve alışverişe çık ve kapat butonlarını göster.

29-Kişi kapat butonuna basarsa iletişim penceresini kapat.

30-Alışverişe çık butonuna basarsa marketin rotasını göster.

31-Akıllı saat ile iletişime geç ve kişinin konumunu öğren.

32-Kişi markete vardı ise alışveriş listesini göster sesli uyarı ver kapat butonunu, tamam butonunu ve haftalık alışveriş listesi butonunu göster.

33-Kapat butonuna basarsa iletişim penceresini kapat

34-Haftalık alışveriş listesi butonuna basarsa yemek tarifleri veri tabanından bir haftalık yemek listesi çıkar

35-Mutfağa bağlan

36-Hazırlanan haftalık yemek listesindeki malzemelerin eksik olanlarını belirle

37-Eksik malzeme listesini türüne göre sırala

38-Saatle iletişime geç

39-Haftalık alışveriş listesini ve kapat butonunu göster.

40-Saatle iletişime geç konumu öğren.

41-Kişi marketten çıkınca iletişim penceresini kapat.

42-Akıllı saatle iletişime geç kişinin uyuyup uyumadığını kontrol et.

43-Kişi uyanıksa 1. Modüle dön.

44-Kişi uyuyorsa programı sonlandır.

45-Bitiş.

Örnek vermiş olduğum algoritmanın şema versiyonları da bulunmaktadır. Fakat bu kadar kapsamlı bir algoritma burada şematize edilemeyeceği için, düz yazı şeklinde adımlar anlatılarak verilmiştir. Üçüncü bölümde ele aldığımız saldırı örnekleri bölümünün Stuxnet başlığında, Stuxnet virüsünün Symantec firması tarafından şematize edilmiş bir algoritması bulunmaktadır.

1.7 YAPAY ZEKÂ

Zekânın sözlükteki karşılığı şu şekildedir: İnsanın düşünme, akıl yürütme, objektif gerçekleri algılama, yargılama ve sonuç çıkarma yeteneklerinin tamamı, anlak, dirayet, zeyreklik, feraset (http://sozluk.gov.tr, 01.07.2019). İnsan zekâsı öğrenebilme kabiliyetine sahiptir. Bu kabiliyeti ile geçmiş deneyimlerden yola çıkarak bir takım çıkarımlarda bulunup, buna göre kararlar verebilmekte ve buna göre hareket edebilmektedir. Örneğin çocuklar sobanın sıcak olduğunu, dokunduklarında kendilerine zarar vereceğini bilmezler, ta ki ilk kez temas edene kadar. Çocuk bunu öğrendikten sonra sobanın sıcak olduğunu, ateşin zarar verici bir şey olduğunu hafızasına kazır. Yapay zekâ ise bu öğrenme ve çıkarımda bulunma mekanizmalarının, bir takım programlama teknikleri ile makineye aktarılmış halidir. Daha öncesinde de bir takım çalışmalar olmakla birlikte, yapay zekâ tartışması ilk olarak Alan Turing tarafından bir İngiliz felsefe dergisi olan “Mind” dergisine 1950 yılının Ekim ayında yazdığı “The İmitation Game” başlıklı makale ile tartışmaya açılmıştır. İnsan aklına benzer şekilde, yapay zekânın temellerinde de yapay öğrenme dediğimiz öğrenen algoritmalar vardır. Amaca göre farklı farklı yapay zekâ algoritmaları bulunmakla birlikte, genel olarak bu algoritmaların amacı olasılıklar uzayından en iyi yolu veya duruma en uygun sonuca götüren yolu bulup, yapay zekânın belleğine kaydetmek üzerine kuruludur. Öğreniyor olması en önemli özelliklerinden

birisidir. Aksi takdirde, edindiği tecrübeleri kullanmayıp sadece tek seferlik sonuçlar vermiş olsaydı, sıradan bir programdan farkı kalmazdı. Peki, sıradan bir programla yapay zekâyı nasıl ayırt ederiz? Yapay zekâ tartışmasını ortaya atan Turing, bir yapay zekâyı sıradan bir makine programından ayırt etmek için bugün halen geçerli olan, Turing testini geliştirmiştir. Turing testinde, bir bilgisayar üzerinden örneğin bir mesajlaşma uygulamasıyla, karşısındaki kişiye sorular soran denek karşısındakinin yapay zekâ mı yoksa insan mı olduğunu anlamaya çalışır. Yapay zekâ ise kendisiyle konuşan deneği, insan olduğuna ikna etmeye çalışır. Eğer denek karşısındakinin bir insan olduğuna ikna olursa, yapay zekâ testi geçmiş olur.

Günümüzde çeşitli alanlarda kullanılan yapay zekâ algoritmalarından birkaç örnek vermek gerekirse:

- *Wall Street'teki işlem algoritmaları(Hisse alım satılarını yapıyor)*
- *Cezai adalet algoritmaları(Trafik lambaları ve radar kameraları, kanun ihlallerini tespit ediyor)*
- *Sınır kontrol algoritmaları (Bir yapay zekâ, sizi ve bagajınızı incelmeye çağırabiliyor)*
- *Kredi puanlama algoritmaları (Kredi notunuzu belirliyor)*
- *Gözetleme algoritmaları(Etrafınızdaki binlerce kamera ile görüntü işleme ve derin öğrenme sayesinde anormal hareketleri tespit ediyor ve yüz taraması yapabiliyor)*
- *Savaş algoritmaları (Hiçbir insan desteği almadan insansız araçların keşif, gözetleme ve imha görevlerini yerine getirmesini sağlıyor.*
- *Aşk algoritmaları(Kişilik özelliklerinizi analiz ederek kusursuz ruh eşinizi bulmayı vaat ediyor)*

  (Goodman, 2016, s:457,458).

Bir diğer önemli örnekse, yapay zekanın sağlık alanında kullanılmasıdır. Akıllı telefonlara indirilecek kadar basitleştirilen uygualamalarla, kalp ve şeker hastalıklarının anı anına izlenmesi sağlanmaktadır. Kola takılan saatler, her gün kaç adım attığınıza varana dek kişisel aktivitelerinizi ölçebilmektedir (Eczacıbaşı, 2018, s: 95). Naiva Bayes algoritması gibi öğrenen algoritmalarla hasta kayıtları veri tabanı, semptomlar, test sonuçları ve hastanın özel bir durumu olup olmadığı gibi bilgiler işlenerek bir saniyeden ksıa bir sürede teşhis koyulabilmektedir. Ve koyulan teşhisler çoğu zaman, tıp fakültesinde yıllarını harcamış uzmanların teşhislerinden daha iyidir (Domingos, 2017, s: 53). Dijital sağlık sektörünün bu tür uygulamalarla 2020 yılına kadar %41 büyümesi beklenmektedir.

1.7.1 Yapay Zekâ Algoritması

Sıradan program algoritmaları iş akışı veya süreç akışı şeklinde iken, yapay zekâ algoritmaları sezgiseldir. Yani belirli bir plan üzerine yürümezler, izleyecekleri yolu kendileri bulurlar. Yapay zekâ algoritmaları arasında, iktisat literatürüne en yakın olanı karar ağacı algoritması olduğundan, burada karar ağacı algoritmasına örnek verilecektir. Karar ağacı algoritmasının temelleri, John Forbes Nash'in 1949 yılında yazmış olduğu 27 sayfalık doktora tezinde öne sürdüğü oyun teorisine dayanır. Oyun teorisi John Nash'a ekonomi Nobel ödülü kazandırmış bir teoridir. Sonrasında oyun teorisi ekonomi alanında geniş yer edinmiştir ve birçok alanda halen kullanılmaktadır.

Oyun Teorisi ve Nash Dengesi

Oyun teorisi, en az iki rakip veya işbirlikçi arasındaki etkileşimi ele alır. Oyun teorisini, en bilinen problemlerinden biri olan mahkûmlar açmazı üzerinden ele alalım:

İki hırsızın, bir banka soygunu sonucunda şüpheli olarak gözaltına alındığını fakat polisin elinde delil olmadığını düşünelim.

Polis, bu mahkûmların her birini ayrı bir sorgu odasına almıştır ve aşağıdaki şu üç teklifi her ikisine de sunmuştur.

1. Eğer her ikinizde itiraf ederseniz 2'şer yıl hapis yatarsınız
2. Sen itiraf etmezsen ve arkadaşın itiraf edip senin aleyhinde tanıklık ederse, arkadaşın serbest kalır sen 4 yıl yatarsın.
3. Eğer her ikinizde itiraf etmezseniz 1'er yıl ceza alırsınız.

Tablo 2: Mahkûmlar Açmazı

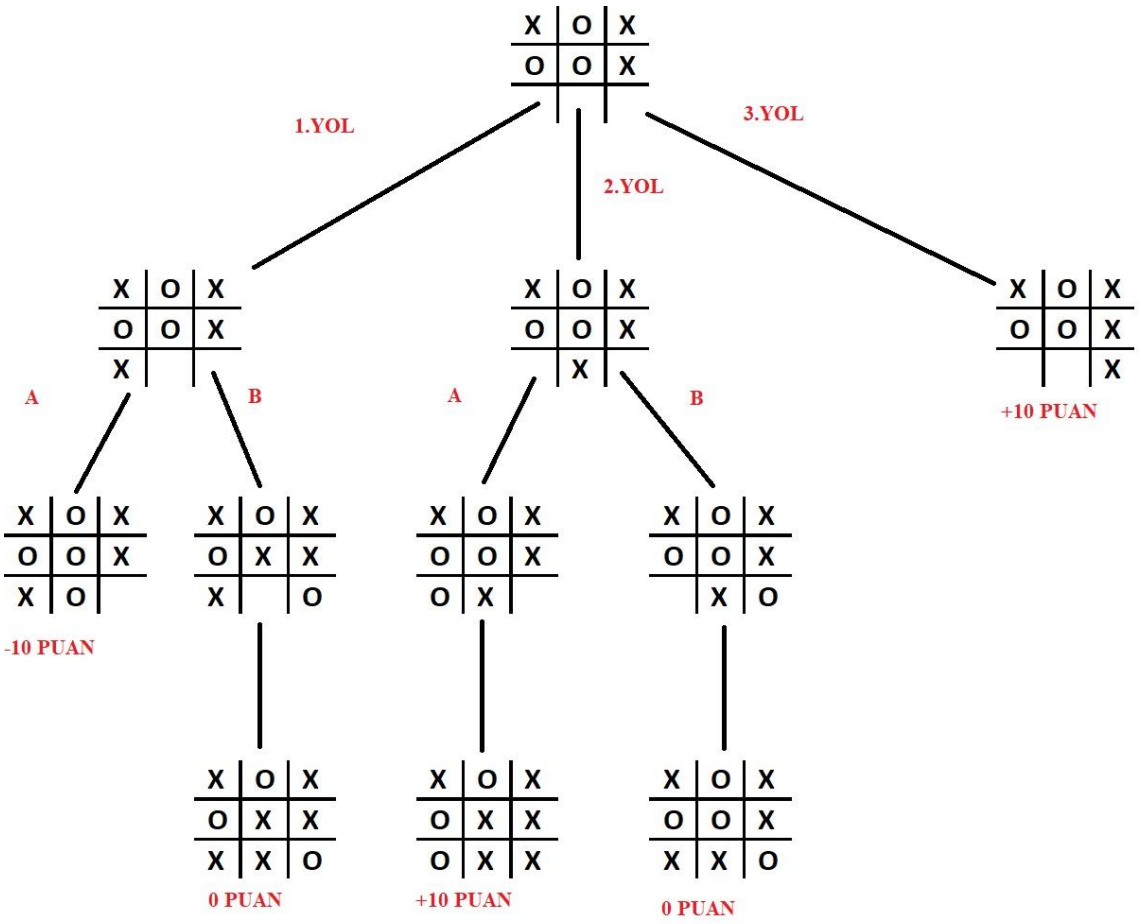
Mahkûmlar	**İtiraf Etme**	**İtiraf Et**
İtiraf Etme	(1'1)	(4,0)
İtiraf Et	(0,4)	(2,2)

Kaynak: Tarafımızdan Oluşturulmuştur

Tabloda görüldüğü gibi bir durum ortaya çıkmaktadır. Bu durumda eğer mahkûmlar birbirleri ile haberleşebilselerdi itiraf etmemeyi seçip 1'er yıl hapisle kurtulabilirlerdi fakat böyle bir şey mümkün olmadığından her ikisi de 4 yıl yatmaktan korkacak ve diğerinin aleyhinde tanıklık ederek itirafçı olacaktır. Bunun sonucunda Nash dengesi 2,2 kümesinde gerçekleşecektir. Nash dengesi bu tür durumlarda en uygun çözümü ifade eder. Örneğimizdeki 2,2 kümesi en iyi çözüm kümesi değildir. Fakat durum

açısından en uygun çözüm kümesidir. Bunun gibi rekabetçi piyasalarda fiyat arttırma veya azaltma problemleri üzerine kurulmuş oyun teorisi örnekleri de vardır.

Karar ağacı algoritmaları da buradan yola çıkarak probleme ilişkin ihtimalleri ele alır ve en iyi sonuca ulaşmaya çalışır. Üçe üç dokuz karede oynanan "tic toc toe" ismindeki oyun üzerinden örnek vermek amacıyla oluşturduğumuz şekil aşağıdadır. Oyunun kuralları gereği her oyuncu sırayla hamle yapar ve üç "X" veya üç "O" yu yan yana getiren kazanır.



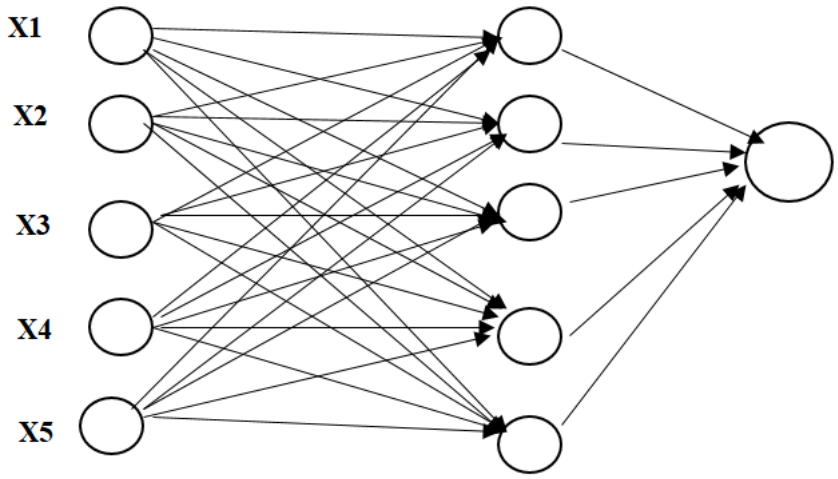
Şekil 4: Karar Ağacı Algoritması
Kaynak: Tarafımızdan oluşturulmuştur

Şekilde görüldüğü üzere, mevcut durumda oyuncunun 3 adet hamle yapma ihtimali var. Bu üç hamleden birinciyi seçtiğinde, karşısına A ve B olmak üzere iki seçenek daha çıkıyor ve sonrasın A'yı seçerse -10 puan B'yi seçerse berabere kalıp sıfır puan alıyor. İkinci yolu izlediğinde ise Gene karşısına A ve B olmak üzere iki seçenek daha çıkıyor ve A hamlesini yaparsa nihai sonuç +10 puan oluyor ve kazanıyor. Eğer oyuncu en başından 3. hamleyi yapmayı seçerse +10 puan alarak gene oyunu kazanıyor.

Bu durumda bu oyun için çözüm kümesi (2A,3) şeklindedir. Yapay zekânın karar ağacı algoritması da bu şekildedir, muhtemel bütün hamleleri hesaplar ve en kısa yoldan en çok getiri sağlayanı tercih eder veya duruma göre en derin tarama da yaptırılabilmektedir. Bu ihtimaller dizisi bir veri seti halinde veri beslemesi olarak yapay zekâya hazır olarak ta verilebilir veya eğitici ile öğrenme modeli izlenerek yapay zekâ bizimle oynadıkça hamlelerin sonuçlarını belleğine kaydederek te öğrenebilir.

1.7.2 Yapay Zekânın Finansal Uygulamaları

Yapay zekânın finansal analizde ilk kullanım örneklerinden birisi Odom ve Sharda'nın 1990 yılında yaptıkları çalışmadır.



Şekil 5: Odom ve Shadra tarafından oluşturulan yapay sinir ağı modeli
Kaynak: Birol Yıldız Finansal Analizde Yapay Zekâ

X1: Çalışma sermayesi/Toplam varlıklar

X2: Kar Yedekleri/Toplam Varlıklar

X3: Vergi öncesi kar/Toplam borç

X4: Öz kaynağın piyasa değeri/Toplam borç

X5: Satışlar/Toplam varlıklar

Oranları kullanılmıştır. Çalışma kapsamında 1975 ve 1982 yılları arasında iflas eden 65 firma ve iflas etmeyen 64 firmanın verileri kullanılmıştır. Modelin çıktı verisi 0 ila 1 arasında bir orandır. Oran 0.5'in altında olduğunda işletmenin iflas edeceği 0.5'in

üzerinde olduğunda işletmenin iflas etmeyeceği doğrultusunda bir tahmin yapılmıştır. Çalışma sonucunda yapay zekâ sinir ağı modeli %81 doğruluk oranıyla iflas eden firmaları tahmin etmişti (Yıldız, 2009, s:134).

Buna benzer bir diğer çalışma da ülkemizde 18 firma ve 18 banka üzerinde modellenerek uygulanmıştır. Araştırma sonucunda yapay sinir ağları analiziyle başarısızlıktan bir yıl öncesi için başarılı ve zarar eden bankalar %100 başarı gücüyle; iki yıl öncesi için ise, başarılı bankalar %77,8, zarar eden bankalar yine %100 başarı gücüyle doğru tahmin edilmiştir (Çelik, 2010, s: 142).

Her ne kadar yapay zekânın kalıcılık, istikrar, belgelendirilebilme, tarafsızlık, verimlilik ve maliyet etkinliği açısından avantajları olsa da dezavantajları da mevcuttur. Yapay zekâ şuan için tasarlanan amaç doğrultusunda uzmanlaşabilmektedir. Fakat insan zekâsı çok yönlüdür, geniş kapsamlıdır. Yapay zekâ yeni bir şey ortaya koyamaz örneğin senaryo yazımı konusunda bunun deneyleri yapılmıştır. Bir yapay zekâya Harry Potter romanının kitapları okutulmuş ve senaryonun devamını yazması istenmiştir. Yapay zekânın ortaya çıkardığı senaryo ise hiçbir açıdan mantıklı bir senaryo olmamıştır. Yapay zekânın finansal uygulamalarında da benzer sıkıntılar yaşanabilmektedir.

Müşteriler adına alım satım kararı alma yetkisine sahip bir tür yapay zekâ olan, yüksek frekanslı elektronik işlem platformları 99'da borsadaki insanların yerini almaya başlamıştır. Sonrasında gelişen süreçte 2015 itibariyle Dow Jones'taki işlem hacminin %70'i yapay zekâya emanet edilmiş durumdadır. Bu yapay zekâ programlarını Rhomson Reuters adında bir haber ajansı 50.000 haber kaynağı ve 4 milyon sosyal medya sitesini hayal edilemeyecek bir hızda tarayarak elde ettiği verilerle beslemektedir (Goodman, 2016, s: 453). Örnekler kısmında da değindiğimiz Syrian Elektronik Army (SEA) isimli hacking grubunun Associated Press gazetesinin Twitter hesabını ele geçirerek "Beyaz Saray'da patlama oldu, obama yaralandı." şeklinde yalan haber yapmaları da işte bu yapay zeka mekanizmalarını harekete geçirmiştir. Bu haberden dolayı terör saldırısı olduğu çıkarımı yapan, yapay zekâ sadece üç dakikada 136 milyar dolarlık satış gerçekleştirmiştir. İşte bu örnekte yapay zekâ teknolojisinin kullanımı esnasında denetim mekanizmalarının ve doğrulama mekanizmalarının çok iyi tasarlanması gerektiğinin aksi takdirde devasa kayıp ve zararlara yol açabileceğinin iyi bir göstergesidir.

1.8 KRİPTOPARALAR & BİTCOİN(BTC)

Kripto para kavramı, kripto ve para kelimelerinin bir araya gelmesiyle oluşmuştur. En bilinen ve ilk örneği Bitcoin'dir. Kriptoloji kısaca şifre bilimidir. Haberleşen taraflar arasında bilgi alışverişinin güvenli olarak gerçekleştirilmesini sağlayan, çoğunlukla temeli matematiksel ifadelere dayanan teknik ve uygulamaların bütünüdür (Bodur, 2016, s:1). Kripto ise şifreli yazı anlamına gelmektedir. Kripto para kavramında çeşitli bilgisayar teknikleriyle elde edilen şifrelerin kendisi para yerine kullanılmaktadır. Elbette bu şifrelerin elde edilmesinde çok güçlü şifreleme teknikleri kullanılarak para, yani şifrenin kırılmazlığı güvence altına alınmaktadır.

1.8.1 Para Kavramının Gelişimi

Para, mal ve hizmetlerin satın alınmasında ve borçların ödenmesinde kullanılan genel kabul görmüş ödeme araçlarıdır. İlk çağlarda fildişi, deniz kabuğu ve bir takım değerli taşlar para olarak kullanılırken sonrasında devletlerin oluşması ile para kullanımı ve piyasada dolaşımı konusunda bir takım düzenlemeler getirilmiştir. Bir nesnenin para olarak adlandırılabilmesi için, bir takım özelliklere ve işlevlere sahip olması gerekmektedir. Örneğin en başta piyasaya süren güvence verecek bir kurum veya kuruluş olmalıdır. Bitcoin'in yasalarımız açısından sadece bir yatırım aracı olarak görülmesinin en önemli dayanağı da dağıtık yapısıdır.

1.8.1.1 Paranın Özellikleri

- **Taşınabilirlik:** Paranın temel kullanım amacı ticareti kolaylaştırmaktır. Bu bakımdan para olarak kullanılacak nesneler de kolaylıkla taşınabilir olmalıdır.
- **Dayanıklılık:** Para aynı zamanda bir değer saklama aracı olduğu için para olarak kullanılacak nesnelerin dayanıklı olması gerekmektedir ki elde edilen ekonomik değeri sorun yaşamadan muhafaza edebilelim.
- **Standardizasyon:** Paranın genel kabul görebilmesi için belirli standartlara sahip olması gerekmektedir. Aksi takdirde kullanılan nesnenin para olup olmadığına dair insanların aklı karışır.
- **Bölünebilirlik:** Gene para kullanımının ilk amacı olan ticareti kolaylaştırması açısından en küçük alışverişlerde dahi kullanılabilecek bir yapıda olması gerekmektedir.

- **Homojen Olma:** Aynı birimi temsil eden her para aynı nakti değere sahip olmalı. Daha iyi anlaşılması açısından, örneğin koleksiyon paralar üzerinde yazılı olan değerden farklı bir değer ihtiva eder. Onlar artık bildiğimiz anlamda para olmaktan çıkmıştır.
- **Genel Kabul Görme:** Paranın değişim aracı olarak kullanılabilmesi için herkes tarafından kabul ediliyor olması gerekmektedir. Burada günümüzde kullandığımız itibari paranın değerinin parayı basan devlete olan güvenle ilişkisi göz önüne alınmalıdır. Günümüzde kullandığımız paralar itibari paradır. Yani parayı basıp piyasaya süren devlete olan güvene göre piyasa da kabul görmektedir. Ekonomik istikrar açısından sorun yaşayan ülkelerin paraları bu yüzden piyasa da değer görmemektedir. Bu durum da o ülkede dolarizasyon denilen duruma sebep olmaktadır. Dolarizasyon bir ülkenin ekonomisinde, ticaretin yerel para birimi yerine yabancı paralarla dönmesidir. Ve ek olarak devletlerin basıp piyasaya sürdüğü paralar devletin piyasaya borcunu ifade eder. Bir bakış açısına göre cebinizdeki 10 lira devletin size olan borcunu ifade eden bir tür kanıttır. Ülkeler arası ilişkilerde de bu durum böyledir. Örneğin bizim merkez bankamızda tuttuğumuz dolar ABD'nin bize olan borcunu ifade eden kâğıtlardır.
- **Taklit Edilememe:** Paranın değer saklayabilmesi için taklit edilememesi gerekmektedir. Taklit edilebildiği takdirde bir değeri kalmaz.

1.8.1.2 Paranın İşlevleri:

- **Takas aracı olma işlevi:** Para aslında ilk devirlerdeki takas ekonomilerindeki takas mekanizmasının işlevini üstlenmiş bir anahtar rolü görmektedir. Mal ve hizmet karşılığında para takas edilir. Ve bu sayede takas ekonomilerinin, takas için ihtiyaç olan malları bulma sorunu ortadan kalkmış olur.
- **Değer saklama işlevi:** Para yapılan işin, verilen hizmetin veya satılan malın bir nevi kanıtıdır. Ekonomide bulunan mal ve hizmetlerin bir karşılığı olarak verilir. Karşılığı olarak verildiği mal ve hizmetin değerini muhafaza eder.
- **Hesap birimi olma işlevi:** Para mal ve hizmetlerin değerlerinin ortak bir birim üzerinden ifade edilmesine olanak sağlar.

1.8.1.3 Paranın Türleri

Mal Para: Mal para takas ekonomileri zamanında kullanılan paradır. Fakat günümüz açısından örnek vermek gerekirse altın bir mal paradır. Değeri üretildiği madene eşit veya yakın olan paralardır.

İtibari Para: Mal olarak bir değer arz etmeyen fakat mal ve hizmetlerin satın alınmasında değişim aracı olarak kullanılabilen her türlü şey temsili veya itibari paradır. Adından da anlaşılabileceği üzere bu tür paralara değerini veren parayı basan veya sunanların verdiği güvence ve itibardır. Bu bağlamda günümüzde devletlerin basıp piyasaya sunduğu günlük yaşamda kullandığımız kâğıt paralar ilk akla gelen itibari paralardır. Mal olarak bir değeri yoktur fakat kâğıt paranın üzerinde yazan değer kadar para işlevlerini yerine getirmektedir.

İtibari paranın kendi alt türleri de şu şekildedir:

-Altın ve Gümüş Sertifikaları: Üzerinde yazılı olan değer kadar altın veya gümüş alacağını temsil eden kâğıtlardır. Banknot sisteminden bir önceki aşamada sıkça kullanılmışlardır. Günümüzde de buna benzer olarak bankalar altın hesapları açmaktadırlar.

-Banknot ve Kağıt Para: Banknot veya kağıt para bugün günlük hayatta kullandığımız kağıt paralardır. Tamamen itibaridir. Yani bu kâğıt paranın geçerliliği devlet otoritesi tarafından veya basan otorite tarafından sağlanmaktadır.

-Madeni Para: Madeni paralar da kâğıt paralar gibi itibaridir ve metal olarak değerlerinden fazlasını muhafaza ederler. Yani eritip metal olarak kullanıldıklarında üzerlerinde yazan parasal değerden daha az değere sahip olurlar.

Kaydi Para: Rezerv yani bankaların ellerinde tuttukları para açısından iki çeşit bankacılık modeli vardır. Birincisi mutlak rezerv bankacılığı, bu modelde bankalar getirilen paraların tamamını ellerinde tutarlar. İkincisi ise kısmi rezerv bankacılığıdır ve bu modelde bankalar belirli bir zorunlu karşılık oranı ayırıp geri kalan parayı kaydi olarak oluştururlar. Örnek vermek gerekirse zorunlu karşılık oranının %20 olarak belirlendiği bir ekonomide herhangi bir bankaya yatırılan 100 lira karşılığında bankalar bu 100 lirayı kasada tutmak şartıyla fazladan 400 liralık işlem yapabilirler. Oluşan 400 liralık fazlalık

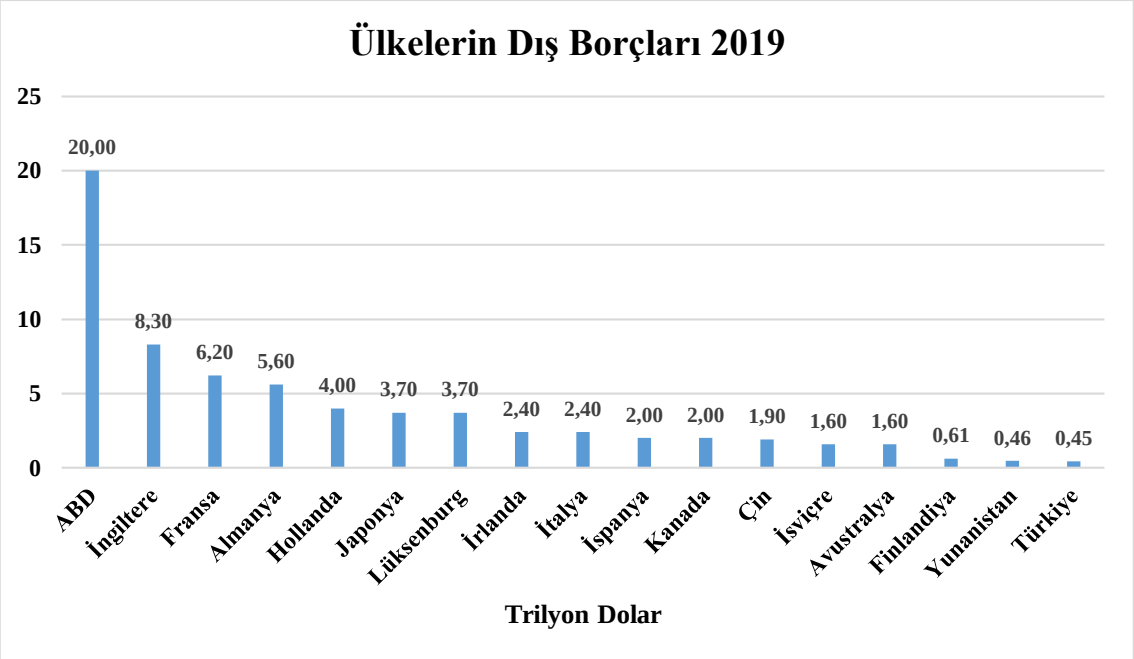
sadece kayıtlarda geçer. Bankaların kayıtlarındaki rakamlardan ibarettir. Kaydi para yalnızca merkez bankası ve bankalar tarafından oluşturulabilmektedir.

1.8.2 Bretton Woods Sistemi

Çok eski devirlerde para olarak çeşitli nesneler kullandıktan sonra değerli metallerin keşfedilmesiyle birlikte altın gümüş gibi değerli metaller kullanılmaya başlandı. Fakat dünyada ticaretin gelişmesi bir takım sıkıntıları da beraberinde getirdi. En büyük sıkıntılardan biri de kilometrelerce yolu deniz ve karadan kat eden ticaret kervanlarını yağmalayan haydutlar ve korsanlardı. Mal almak üzere üzerinde yüklü miktarda altın veya gümüşle yola çıkan tüccarlar yolları kesilerek soyulmaya başladığında, bir çözüm geliştirme yoluna gittiler. Bu çözüm gittikleri ticaret şehirlerinde güvenilir kişilere altın ve gümüşlerini emanet etmekti. Emanet ettikleri bu altın ve gümüş karşılığında üzerinde miktarını ve emanet alan kişinin bilgilerinin yazdığı bir kâğıt alıyorlardı. Böylece yolda soyulma riskinden kurtuluyorlardı. Ödemelerini de bu kâğıtla yapıyorlardı. Yani ticaret tüccar, satıcı ve altınları tutan kişiler arasında üçlü bir takasla yürüyordu. Altın ve gümüş gibi değerli metalleri emanet alan kişilere bu işlemleri yaptıkları esnada üzerinde oturdukları banktan dolayı zamanla banker denilmiştir. Sonrasında gelişen süreçte bankerler ellerinde bulunan altın rezervinden daha fazla altın sertifikası dağıtmaya başlamışlardır yani kaydi para oluşturmaya başlamışlardır. Bir düzenleme olmaksızın oluşturulan kaydi para sonucunda bazı ekonomik sıkıntılar baş göstermiştir. Ve devletler bankerlerin ekonomi üzerindeki güçlerini keşfederek bu işlere bir düzenleme getirmeye başlamıştır. Bunun sonucunda da ilk merkez bankaları ortaya çıkmıştır. O zamanlarda insanlar ellerindeki değerli metalleri bu bankalara götürür karşılığında da para alırlardı. Verilen para kadar altın ve değerli metal de bankada tutulurdu.

Fakat gelinen nokta ve sağlanan bütün bu kolaylıklar da yeterli olmamıştır. Devletlerin merkez bankalarının para basarak elde ettikleri kaydi paraya senyoraj geliri denilmektedir. Uluslararası ticaretin yürütülebilmesi için merkez bankaları ellerinde belirli miktarlarda diğer ülkelerin para birimlerini de rezerv olarak bulundururlar. Elde tutulan bu yabancı paralar, parayı basan ülkenin parayı elinde bulunduran ülkeye olan altın borcu miktarını ifade etmekteydi. Fakat birinci dünya savaşı ve ikinci dünya savaşı

gibi büyük savaşların baş gösterdiği yıllarda devletler finansman için aşırı bir şekilde kaydi para oluşturmuşlardır. Savaşa giren ülkenin kaderinin belli olmaması ve piyasada artan kaydi para miktarından dolayı paranın değeri tartışılır olmuştur. İkinci dünya savaşının sonlarına doğru 1944 Temmuz'unda ABD'nin New Hampshire eyaletinin Bretton Woods kasabasında, 44 ülkenin katılımı ile gerçekleştirilen toplantıda uluslararası para sisteminin kuralları belirlenmiştir. Alınan karara göre bütün katılımcı ülkeler, paralarını dolara endeksleyecek ve ABD doları da (35$ = 1 ons altın) şeklinde altına endekslenecektir. Diğer bir deyişle ABD bastığı her 35 dolar karşılığında 1 ons altını rezervinde bulunduracaktır. Bretton Woods sisteminin yürümesi için International Monetary Fund (IMF) World Trade Organization (WTO) ve World Bank (WB) kurulmuştur. Başlarda sistem sorun çıkarmadan işlemiştir. Fakat 1970'lere gelindiğinde ABD'nin bütçe açığı ödenemeyecek noktaya gelmiştir. Yani ABD elinde bulundurduğu altından kat ve kat fazla dolar basmıştır. 1971 yılında dönemin ABD başkanı Robert Nixon yaptığı bir açıklamayla doların artık bir altın karşılığı olmadığını açıklar. Fakat kurulu düzen çeşitli düzenlemeler ve kurtarma operasyonlarıyla günümüze kadar bu şekilde sürmeye devam eder.



Grafik 10: Ülkelerin Dış Borçları 2019
Kaynak: Ceicdata

Grafik 10'da ülkelerin güncel dış borçlarını görmektesiniz. ABD'nin dış borcu 20 trilyon dolar seviyesindedir. Kendisine en yakın İngiltere, Fransa ve Almanya'nın dış

borçları toplamından da fazla dış borcu vardır. Bunu mümkün klan Bretton Woods sistemidir. Özetleyecek olursak mevcut durumda hemen hemen dünyadaki tüm ülkeler uluslararası ticarette ve ihtiyat amacıyla rezerv para olarak merkez bankalarında dolar tuttukları için, teknik olarak ABD bütün dünya ülkelerinin dış borç potansiyeli kadar dış borçlanmaya gidebilmektedir. Başka bir ifadeyle ABD sadece kağıdı yeşile boyayıp dolar basarak karşılıksız olarak gelir elde etmektedir. Bu bozuk düzen ne kadar ayakta tutulmaya çalışılsa da zaman zaman krizlerle ekonomileri çökme noktasına getirmektedir.

Tablo 3: 2007 ve 2008 Küresel Kriz Döneminde Büyük Finansal Kuruluşlara Kaynak Sağlayan Ulusal Varlık Fonları

TARİH	**ÜLKE**	**FON**	**FİNANSAL KURUM**	**YATIRIM TUTARI (Milyar USD)**
Mayıs 2007	Çin	China Investment Corporation	BLACKSTONE GROUP	3.0
Temmuz 2007	Singapur	Temasek Holdings	BARCLAYS	2.0
Kasım 2007	BAE	Abu Dhabi Investment Authority	CITIGROUP	7.5
Aralık 2007	Singapur	Goverment Investment Corporation	UBS	11.5
Aralık 2007	Çin	State Administration of Foreign Exchange (SAFE)	MORGAN STANLEY	5.0
Aralık 2007	Singapur	Temasek Holdings	MERRILL LYNCH	4.4
Ocak 2008	Singapur	Goverment Investment Corporation	CITIGROUP	6.9
Ocak 2008	Kuveyt	Kuwait Investment Authority	CITIGROUP	3.0
Ocak 2008	Güney Kore	Korea Investment Corporation	MERRILL LYNCH	2.0
Ocak 2008	Kuveyt	Kuwait Investment Authority	MERRILL LYNCH	2.0
TOPLAM				**47.3**

Kaynak: AKBULAK, Sevinç& AKBULAK, Yavuz, Marmara Üniversitesi, İ.İ.B.F Dergisi, Yıl 2008, Sayı 2, s 243

Tablo 3'te ise bu bozuk parasal düzenin neden olduğu 2008 krizinde ABD'nin büyük şirketlerine fon sağlayan ulusal varlık fonlarını görmektesiniz. Bu tür müdahalelerle sistem ayakta tutulmaya çalışılmaktadır. Günümüzde dolara endeksli ekonominin tıkandığını düşünen veya bu tür sorunlardan mağdur olan ülkeler kendi aralarında yerel ekonomik gruplaşmalar oluşturmaktadır. Çin ve Rusya ticaretlerini yerel paralar üzerinden yürütme kararı almışlardır. Aynı şekilde Türkiye de Rusya ile ve daha pek çok ülke ile yerel para birimleri üzerinden ticaret antlaşmaları yapmaktadır. Dolar cephesinin dağılmaya başladığı söylenmektedir. Bu durumda ekonomik sebeplerin etkisi olduğu kadar, ABD'nin elindeki dolar basma yetkisini uluslararası arenada çıkarlarının ters düştüğü ülkelere karşı adeta ekonomik bir silah olarak kullanmasının da etkisi yadsınamaz.

1.8.3 Ödeme Sistemleri

MÖ. 9000'lerde atalarımız nesneleri değiş tokuş ederek ihtiyaçlarını karşılamaya başlamasıyla trampa ekonomisi denilen takas ekonomisi oluştu. Fakat takas ekonomisinin bazı zorlukları vardı. Örnek vermek gerekirse birinin süte ihtiyacı var, elinde ise süt ile takas etmek için et var, başka birisinin de mızrağa ihtiyacı var ve takas etmek için elinde süt var. Bu durumda bu iki kişiden birisinin gidip elindeki sütü veya eti mızrakla takas edebilecek üçüncü bir kişiyi bulması gerekmektedir.

> *Takas ekonomisinin ihtiyaçları karşılamakta etkin olmaması üzerine MÖ. 3000'lerde Babil döneminde tabletlere yazılı bir takım ticaret kuralları geliştirilmiştir. Bu kuralar da yeterli olmayınca MÖ. 1200'lerde nadir deniz kabukları mal para dediğimiz bir tür para olarak kullanılmaya başlanmıştır. Para yerine deniz kabuğu ile ticaret yürütülmeye çalışılmıştır. MÖ. 1100'lere gelindiğinde ise deniz kabuklarının yerini değerli metal parçaları almıştır ve ilk kez Çin'de takas için kullanılmıştır. MÖ. 600'lerde ise Lidyalılar ilk kez değerli metallerden para basmışlardır. 1250'de Floransa'da Florin adı verilen altın sikkeler Avrupa'ya yayılmıştır. 1260'da Moğol hükümdarı Kubilay Han'ın tarihte ilk kez kâğıt banknotu bastırmıştır. 1368'de Floransa'da ilk kez bir bankaya çek ile ödeme talimatının verilmiştir.1609'da İlk modern merkez bankası Amsterdam'da kurulmuştur.1661'de İsviçre'de kâğıt banknotlar resmen basılmıştır.1696 İngiltere'de Isaac Newton ilk seri sikke basan makineyi geliştirmiştir. 1871'de İlk kez Western Union tarafından elektronik fon transferi (EFT) işlemi yapılmıştır.1944'de Bretton Woods Anlaşması yapılmış, IMF ve Dünya Bankası kurulmuş ve altın standardı benimsenmiştir. 1949 Diners Club adı ile ilk kartlı ödeme sistemi hayata geçirilmiştir. 1965'te çek takas sistemini hayata geçirilmiştir.1971'de altın standardı yürürlükten kaldırılmıştır. 1973'de SWIFT sistemi kurulmuştur. 1976'da Visa ödeme şemasının doğmuştur. 1979'da Mastercard ödeme şeması doğmuştur. 1985'te ilk modern ATM cihazları kullanılmaya başlanmıştır. 1995'te debit kartlar kullanıma sunulmuştur.1999'da İlk kez cep telefonları ile temel bankacılık servisleri başlamıştır. 2005'te PayPal kurulmuştur. 2006'da Avrupa'nın ilk temassız kartı Türkiye'de kullanıma girmiştir. 2007'de Afrika'da M-Pesa hizmete girmiştir. 2008'de İngiltere'de temassız kartlar kullanılmaya başlanmıştır. 2009'da İlk mobil banka uygulamaları kullanılmaya başlamıştır. 2009'da Bitcoin Blockchain ağı çalışmaya başlamıştır. 2014'te Apple Pay'in hayata geçmiştir*(Usta, 2019, s: 14).

Ödeme sistemlerinin tarihsel gelişimi yukarıda anlatıldığı gibi olmuştur. Günümüzdeki mevcut ödeme sistemlerinin belli başlı sorunları bulunmaktadır. Mevcut ödeme sistemlerinin en temel sorunu, ödeme sistemlerinin bankalar veya aracı kurumlara bağlı olması, merkezlerinde de bulundukları ülkenin ticaret kanunları ve merkez bankları bulunmasıdır. Bu merkezi kurumlar ülkelerin politikaları doğrultusunda işletildiği için

zaman zaman uluslararası ticarette tıkanmalara yol açabilmektedirler. Wikileaks konusunda değindiğimiz PayPal, Maestro ve Visa gibi aracı kurumların ABD'nin politikalarını izleyerek Wikileaks'e karşı tavır alması ya da Yunanistan krizinde Yunan hükümetinin banka mevduatlarının %10'luk kısmına el koyması bunun en iyi örneklerinden biridir. Bu tür olaylar ödeme sistemleri ve aracı kurumların hükümetlerin kontrolünde olmasını sorgulanır hale getirmiştir.

1.8.4 Bitcoin Madenciliği

> *New York'ta 31 Ekim 2008 saat 14:10'da belirsiz bir e-porta listesinde yer alan ve kriptografi uzman ve meraklılarını içeren yüzlerce üye kendisine Satoshi Nakamoto diyen birinden bir e-posta aldı. Nakomoto mesajında, güvenilir bir üçüncü tarafa ihtiyaç duymadan tamamen karşılıklı olarak çalışacak yeni bir elektronik para sistemi üzerinde çalıştığını yazmıştı kısa açıklamayı okuyanları satın aldığı bitcoin.org adında bir web sitesinde bitcoin olarak adlandırdığı bir para birimi sistemi açıklayan dokuz sayfalık rapora yönlendirmekteydi(Vigna & Casey, 2017, s:66).*

Bitcoin sistemi bu şekilde başlamıştır. Nakamoto'nun bitcoin algoritması 64 karakter uzunluğunda hash(özet şifre) üreten SHA-256 denilen bir şifreleme sistemini kullanmaktadır. Örnek bir hash dizisi şu şekilde alfa numerik olarak oluşturulmaktadır.

Bir SHA-256 hash örneği:

22f80d570c7c4c303d21ec0c008385978697256521f1278350e18aae39dcb13d

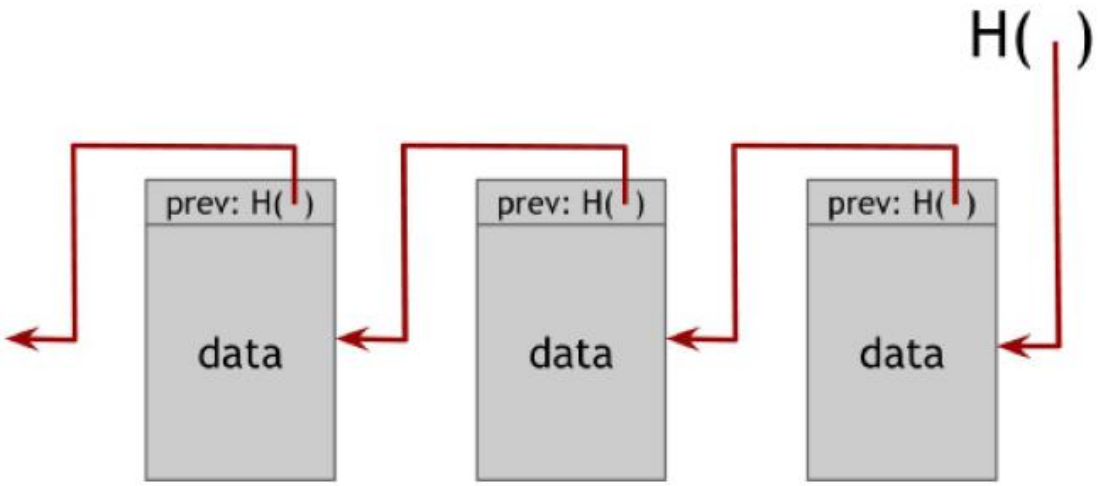
Bu şekilde şifrelenmiş olan bitcoin bilgileri bloklar aracılığıyla dağıtık yapıda iletilir.

Bir transfer işlemi başlatıldığında bloklar arasında iletilen veri şu şekildedir:

Current Depth	10
Block Size (bytes)	948,466
Nonce	2541438316
Merkle Root	141fd6c9e533fa34c0831c9be7f745ca60bb45d4c47fba85720bbdc6877eeaed
Bits (difficulty target)	387,911,067
Version	536870912
IP Relayed By	209.97.148.196:8333

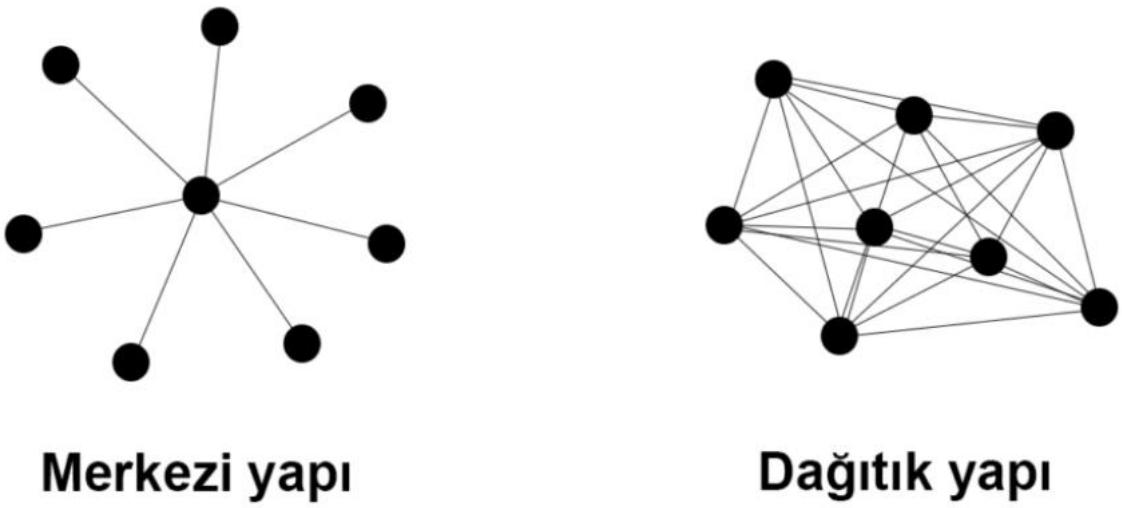
Şekil 6: Bitcoin transferi esnasında şifrelenerek gönderilen bilgiler.
Kaynak:live.blockcypher.com/btc/block/

Blokların birbiri ardına eklenmesi ile aşağıda şekil 7'de görülen blok zinciri oluşur. Blok zincirinin birleşimi ile de dağıtık bir yapıda olan bitcoin ekosistemi oluşur.



Şekil 7: Blok zinciri veri yapısı
Kaynak: Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri, Ersin Ünsal, Ömer Kocaoğlu

Bitcoin madenciliği de tam olarak bu noktada devreye girmektedir. Bitcoin kazanmak için internetten bitcoin madenciliği programı indirip çalıştırdığımız anda, biz de şekil 8'de görülen dağıtık yapıya katılmış oluyoruz. Program Nakamoto'nun algoritmasıyla işlemci gücünü kullanarak hash üretmekte ve transfer işlemlerini ve kayıtları şifreleyip kaydetmektedir. Belirli bir işlem sayısından sonra da komisyon olarak blok zincirinde bulunan madencilere belirli miktarlarda bitcoin vermektedir.



Şekil 8: Merkezi Yapı ve Dağıtık Yapı
Kaynak: coin.hwp.com.tr/blockchain-nedir-nasil-calisir

Bütün bu güvenlik işlemlerine ek olarak bitcoinin birde çoklu imza escrow sistemine benzeyen bir güvenlik önlemi daha bulunmaktadır. Escrow kelimesi Fransızca'da bir parça kâğıt anlamına gelen "escroue" kelimesinden gelmektedir. Escrow sistemi gittigidiyor, hepsiburada gibi sitelerden tanıdık olduğumuz bir mekanizmadır. Alıcı parayı ödediğinde sitenin hesabına ödeme yapmış olur. Mal eline ulaşınca ödemeyi onaylar ve para site tarafından satıcıya aktarılır. Bu sistemin alıcı, satıcı ve aracı site tarafından anahtarla (3'lü) onaylanmasına çoklu imza escrow denir. Bitcoinde de benzer bir havuz sistem vardır. Belirli bir sayıdaki transferleri geçici adreslere alarak orada karıştırıp işlemler onaylanınca alıcılara göndermektedir. Bu sayede kimin nereye transfer yaptığını öğrenmek imkânsız hale gelmektedir.

Aynı zamanda bitcoinin bir de yarılanma süresi bulunmaktadır. Nakomoto'nun algoritması her 4 yılda bir 210.000 blok üretiminden sonra blok üretim hızı yarıya düşürülecek şekilde ve üst limit olarak ta 21 milyon blok olacak şekilde tasarlanmıştır. Yani her 210 bin bitcoin üretildikten sonra veya her 4 yıldan sonra üretim hızı yarıya düşecek ve nihai olarak 21 milyon bitcoin üretildiğinde üretim duracaktır.

Bitcoin üretmenin gittikçe zorlaşan yapısı bitcoin madencilerini değişik teknikler arama yoluna itmiştir. Bu tekniklerden en genel kullanılanı bitcoinin piyasa sürülme evresi olan genesis bloğunun üretiminde Nakamato'nun topladığı yazılım uzmanlarından birisi olan Laszlo Hanyecz tarafından geliştirilmiştir. Hanyecz bitcoin madenciliği programında yaptığı bir takım düzenlemelerle bitcoin çıkarma işlemini Merkezi İşlemci Ünitesi (CPU) yerine gene bilgisayarlardan tanıdık olduğumuz Grafik İşlemci Ünitesi (GPU) ile çıkarmaya başlamıştır. Grafik işlemciler veya tanıdık adıyla ekran kartları görüntü işlemeye yönelik tasarlanmışlardır ve CPU'lardan kat kat fazla aritmetik mantık birimleri(çekirdekleri) vardır. Bu sebeple merkezi işlemcilerine göre çok fazla işlemi aynı anda yapabilirler. Grafik işlemcilerin bu yapısı ve Hanyecz'in yaptığı düzenlemeler sayesinde başlangıca göre çok daha hızlı bitcoin çıkarılmaya başlanmıştır. Bu teknik bitcoin madencileri arasında yayılmış ve GPU'ları paralel bağlayarak daha çok işlem gücü ile daha hızlı bitcoin çıkarılabilen özel tasarımlara dönüşmüştür. Bu dönüşüm adeta bir silahlanma yarışı gibi bilgisayar piyasalarını alt üst etmiştir.

İlk Bitcoin Harcaması

İlk bitcoin harcaması 21 Mayıs 2010'da GPU'ları bitcoin madenciliğine kazandıran Laszlo Hanyecz tarafından gerçekleştirilmiştir. Geliştirdiği teknik sayesinde elinde çok fazla bitcoini olan Hanyecz bitcoin forumlarından birinde bir teklif sundu. İki adet büyük boy pizza karşılığında 10.000 bitcoin teklif etti. O güne kadar bitcoin ödeme yöntemi olarak kullanılmamıştı bir İngiliz vatandaşı bu teklifi kabul etti ve kredi kartıyla ödeme yaparak ABD'de bulunan Laszlo Hanyecz'in adresine pizza sipariş etti. Hanyecz'de 10.000 bitcoini onun bitcoin cüzdanına gönderdi. 10.000 bitcoin o zamanki değeri ile yaklaşık 41 $ ettiği düşünülüyordu (Vigna & Casey, 2017, s:117).

1.8.5 BTC Bilgisayar Pazarı Krizi

Grafik 11: Bitcoin Madenciliğinin Bilgisayar Sektörüne Yansıması
Kaynak: Statista, https://www.statista.com/chart/15843/nvidia-and-radeon-gpu-pricing/

Bitcoin madenciliği başlığı altında değindiğimiz gibi GPU'lar yani ekran kartları yapısı itibariyle bitcoin madenciliği için elverişli olduklarından piyasa da aşırı şekilde GPU talebi oluşmuştur. Bitcoin madenciliğinin yaygınlaşması üzerine de herkes GPU

alıp bitcoin madenciliği yapıp ne kadar sürede harcadıkları parayı amorti edecekleri hesabına girişmiştir. Durum böyle olunca GPU talebi bir çığ gibi büyümüş piyasa da GPU bulmakta zorluk çekilmeye başlanmıştır. Bunun üzerine iktisadın en temel kaidesi gereği artan talep GPU fiyatlarını da arttırmıştır. GPU fiyatlarındaki artış ve bir anda bu kadar çok işlem gücünün bitcoin ekosistemine girmesi, bitcoinin algoritmasının yapısından dolayı rekabeti arttırmıştır. Bitcoin yarışı giderek daha pahalı hale geldiği için insanlar yatırımlarını tekrar gözden geçirmiştir. GPU'ların kendisini amorti etme süresinin uzadığını görmüşlerdir. Bunun sonucunda da ilerleyen süreçte GPU'lara olan talep azalmış ve fiyatlar normale dönmüştür. Pazar araştırma firması olan Jon Peddie firmasının 2018 raporuna göre, 2017 yılında madenciler tarafından 3 milyondan fazla GPU satın alınmıştır. GPU üretici firmalarından en çok tercih edilense AMD marka GPU'lar olmuştur. 2017 yılında AMD 776 milyon dolarlık GPU satışı gerçekleştirmiştir.

1.8.6 Korsan Madencilik Ve İlk Bitcoin Hırsızlığı

Bitcoin konusunda yaşanan gelişmeler, farklı farklı bitcoin madenciliği metotlarının gelişmesine neden olmuştur. Elbette kara şapkalı hackerlar da paranın kokusunu aldıklarında izlemekle yetinmemişler ve harekete geçmişlerdir. Hackerlar geliştirdikleri reklam virüsü tarzındaki programlara bitcoin madenciliği kodları yerleştirerek çeşitli bulut servislerinde ya da trafiği yoğun sitelerde bu virüsleri yayıyorlar. Sonrasında virüs siteyi ziyaret edenlerin bilgisayarlarına bulaşıyor ve bulaştığı bilgisayarların işlem gücünü fark ettirmeden kullanarak bitcoin madenciliği yapıyor. Hackerların korsan madencilik için başvurduğu bir diğer yöntem de kalabalık ortamlardaki, kafe restoran vb. yerlerdeki kablosuz ağlarda bu tür yazılımları yayarak ağa bağlanan telefon ve bilgisayarlara bu tür kriptopara virüsleri bulaştırmak.

İngiltere Bilgi Komisyonu Ofisi (ICO),hackerlar tarafından sitelerine eklenen zararlı yazılımla ziyaretçilerin bilgisayarlarına sızıldığı ve kripto para madenciliği yapıldığı gerekçesiyle web sitesini erişime kapattı. ICO'nun sitesini geçici olarak erişime engellemesi, söz konusu siber tuzağın boyutlarını ortaya çıkardı. Güvenlik araştırmacısı Scott Helme, ICO'nun tuzaklı tek web sitesi olmadığını; aralarında devlet kuruluşlarına ait olanların da yer aldığı 4.000 stenin benzer zararlı yazılımlara sahip olduğuna dikkat

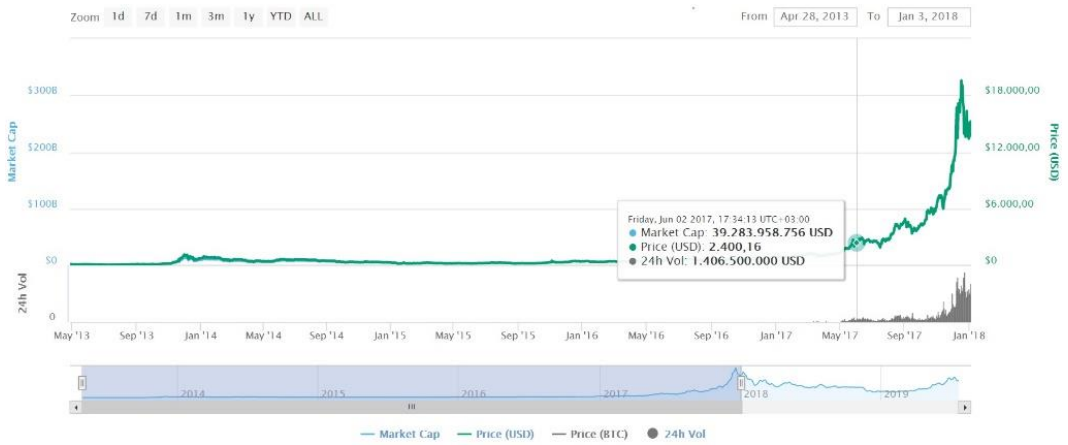
çekti(https://www.haberturk.com/siber-korsanlar-4000-siteye-izinsiz-madencilik-yapan-zararli-yazilim-yerlestirdi-1834257-ekonomi, 1.5.2019).

Örnek verdiğimi haber ve benzeri olaylar pek çok açıdan incelenmesi gereken konulardır. Çoğu zaman bilgisayarlara bulaşan virüsler dosyalara zarar vermedikçe insanlar tarafından bir maliyet olarak görülmemektedir. Fakat örneğimizde görüldüğü gibi tam olarak bir maliyeti olan bir virüs. Örnekteki saldırının ilk dalga ekonomik etkisi, saldırganın sizin cihazınızın işlemci gücünü kullanarak elde ettiği bitcoin miktarı kadardır. Eğer saldırgan bu işlemci gücünü kullanmasaydı belki de siz kullanarak o miktarda bitcoin elde edip bunu paraya dönüştürecektiniz. Görünüşte cebinizden bir şey çıkmadı belki fakat potansiyel kazanımlarınızı çaldırmış oldunuz. Bu ilk dalga etkinin devamında gelişin zincirleme bazı kayıpların yaşanması da mümkündür elbette. Bilgisayarınızın aşırı çalışmadan dolayı çökmesi, yetiştirmeye çalıştığınız işlerin bilgisayarın yavaşlamasından dolayı aksaması, aşırı güç tüketiminden dolayı bilgisayarınızın bataryasının ömrünün bitmesi gibi birbiri ardına gelişebilecek bir takım zincirleme etkileri de göz önünde bulundurmak gerekmektedir.

Bitcoinler cüzdan denilen platformlarda kayıt altına alınırlar. Bitcoini bir kağıda yazıp da saklayabilirsiniz fakat tıpkı kullandığımız paranın bankada durması pek çok kullanım kolaylığı getirdiği gibi uzun alfa numerik karakterler dizisinden oluşan bitcoini de sanal ortamda saklamak pek çok kullanım kolaylığı getirmektedir. Her şeyde olduğu gibi bu konuda da kullanım kolaylığı arttıkça beraberinde riskleri de getirmektedir. İşte bu bitcoin cüzdanlarından biri olan Mt.Gox sitesi 13 Haziran 2011 tarihinde bir hacker tarafından hacklenip yaklaşık yarım milyon bitcoin çalınmış ve alım-satım formlarında tanesi bir peniden satılmıştır. Bunun sonucunda da o tarihlerde 17$ olan bitcoinin değeri sentlere düşmüştür (Vigna & Casey, 2017, s:123).

1.8.7 BTC Çin Krizi

Sosyal medya konusunda olduğu gibi para konusunda da Çin'in baskıcı rejimi ters tepmiştir. Çin 1 Temmuz 2017'de yurt dışına para gönderimine kota getirdi. Çin'in çıkardığı yasaya göre 40.000 Yuandan fazla olan yurt dışı para akışları devlet takibine alınacaktı. Çin'in uyguladığı yasak sonucunda bitcoine aşırı talep oldu ve grafik 12'de görüldüğü üzere bitcoin hızla yükselmeye başladı.

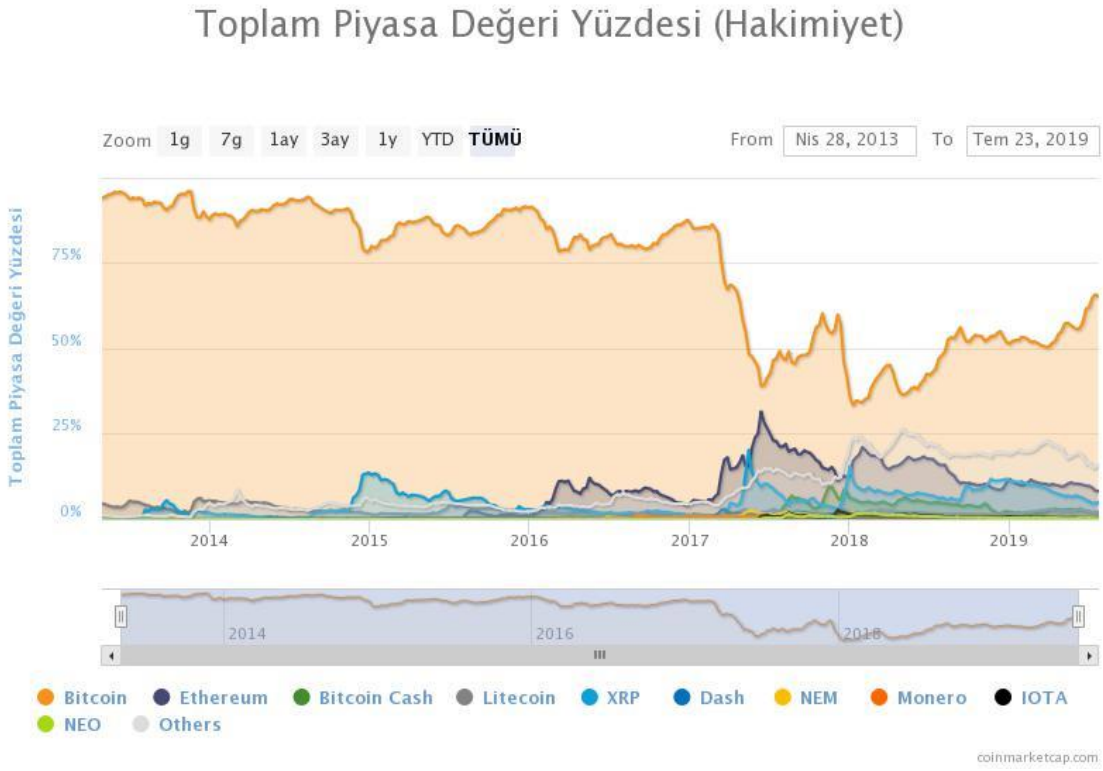


Grafik 12: Çin'in Para Dolaşımını Kısıtlaması Sonrası BTC
Kaynak: (Aksoy, 2018, s:71)

Bitcoin ve Çin Krizi örneğinin ekonomi literatürü açısından önemi Çin hükümetinin para politikası uygulayamamış olmasıdır. Bitcoinin merkezi olmayan, dağıtık yapısından dolayı kontrolü mümkün olmamaktadır. Bu durum da hükümetlerin bitcoine karşı tavır almalarına neden olabilmektedir.

1.8.8 Bitcoin Ve Alternatif Kriptoparalar

Bitcoin dışındaki kriptoparalara alternatif coinler denilmekte ve kısaca altcoin olarak bahsedilmektedir. Altcoinlere yatırım yapmak için önce bitcoin alıp sonra da bu bitcoini yatırım yapmak istediğiniz altcoin türüne çevirmeniz gerekmektedir. Bu durumun ve ilk kriptopara olmasının avantajlarından dolayı bitcoin, piyasada hâkimiyetini sürdürmektedir.



Grafik 13: Bitcoin Piyasa Hakimiyeti
Kaynak: Coinmarket coinmarketcap.com/tr/charts/

Grafik'13 de görüldüğü gibi zaman zaman dalgalanmalar olsa da, zamanla piyasa hâkimiyeti azalsa da, genel olarak kriptopara pazarına bitcoin hâkimdir. Grafik'13 de ikinci sırada görülen Ethereum'un başarısı ise arkasındaki Microsoft, IBM, JPMorgan gibi güçlü firmaların desteğinden kaynaklanmaktadır. Ethereum'un çıkarılış amacı bitcoine rakip olmaktır ve bu doğrultuda bir strateji izlemektedir. Şimdilik bitcoinden aldığı, pazar payı oranları ile başarılı olduğu söylenebilir. Ethereum'dan sonra gelen Bitcoin Cash ise, bitcoin algoritmasının katı sınırlamalarından dolayı tıkanan bitcoin sistemine akış sağlamak için 1 Ağustos 2017 yılında piyasaya sürülmüştür. Pazar payının yüksek olması da gene bitcoine dayanan itibarından kaynaklanmaktadır. Gene en çok bilinen kriptoparalardan olan grafik 13'de dördüncü sırada gelen LiteCoin ise eski bir Google mühendisi olan Charless Lee tarafından bitcoine rakip olması için hazırlanmıştır. Litecoinin bu denli yayılmasının sebebi ise bitcoin'den sonra çıkan ilk alternatif coin olmasından ve bitcoinin değeri çok yüksek olduğu için litecoinin değerini belirli bir seviyede tutarak küçük işlemlere izin veren yapısından kaynaklanmaktadır. Bitcoinin pazar payını kaybetmesindeki bir diğer önemli etken ise en değerli ve ilk kriptopara olmasından dolayı sık sık siber saldırılara maruz kalmış olmasıdır.

Kriptoparalar ülkelerin de dikkatini çekmektedir. Estonya, Rusya, İsveç, Japonya listeye yeni eklenen ülkemiz Türkiye ve daha pek çok ülke kendi kripto paralarını çıkarmayı planlamaktadırlar. Kendi kriptoparasına sahip ülkelerse şimdilik Venezuela ve Dubaidir. Venezuela'nın kriptoparası Petro, Dubai'nin kriptoparası Emcash'tir ve her iki ülke de kripto paralarını 2017 yılında çıkarmışlardır.

Kriptoparaların Ülkeler Açısından Yasal Durumu: ABD, Avustralya, Estonya, Güney Kore, Finlandiya, Hollanda, Kanada, Japonya, İsveç ve İngiltere'de kriptoparaların durumu, yasal olarak düzenlenmiştir. Türkiye, Danimarka, Ukrayna Rusya ve Vietnam'da ise kriptoparaların durumu, henüz yasal bir çerçeveye oturtulmamıştır. Ekvator, Fas, Bolivya, Kırgızistan ve Bangladeş'te ise Kriptoparalar yasaklanmıştır.

1.8.9 Bitcoin aslında nedir?

Çin örneğinde ve daha pek çok ülkede olduğu gibi, ülkemizde de bitcoin 6493 sayılı ödeme sistemlerini düzenleyen kanun kapsamında elektronik para veya bir ödeme aracı olarak görülmemektedir. Bitcoinin ödeme aracı olarak kabul edilmemesine dair en önemli dayanak herhangi bir resmi kurum veya özel kuruluş tarafından ihraç edilmiyor olmasıdır. Dolayısıyla güvence verebilecek bir tarafın bulunmamasıdır. Fakat riskli olmakla birlikte bitcoin bir yatırım aracı olarak değerlendirilebilmektedir. Birçok ülkede de statüsü bu şekildedir. Bitcoin hakkındaki bir diğer görüş te Dr. Ramazan Kurtoğlu'nun "Psiko Siber Savaş ve Küresel Para Oyunları" eserinde detaylıca ele aldığı küresel sermaye baronlarının bitcoini planlamış olabileceği görüşüdür. Bu doğrultuda gene bitcoinin dağıtık ağ yapısı Pentagon tarafından geliştirilmiş olan Tor Ağı'nın dağıtık yapısına benzerlik göstermektedir. Bu açıdan bakıldığında bitcoinin ABD'nin dış borçlarını kapatmak için veya yeni bir parasal düzen kurmak için şişirilen bir balon olabileceği düşüncesini akıllara getirmektedir. Bitcoin hakkında tartışılması gereken bir diğer konu da bitcoin ekosisteminde elden ele şifrelenerek dolaştırılan verilerin, aslında ne olduğudur.

Pedro Domingos "Master Algoritma" adlı eserinde Master Algoritma'yı hayatın tüm akışını verebilecek bir algoritma olarak tanımlamaktadır. Gene aynı doğrultuda Faruk Eczacıbaşı "Daha Yeni Başlıyor" adlı eserinde gelecekte telefonlarımızda bulunan dijital asistanların daha da geliştirilip yapay zekâ ile desteklenerek, bizim bir dijital ikizimizin oluşturulabileceğinden bahsetmektedir. Bütün bu tartışmalar ilk bakışta felsefi

bir tartışma gibi gözükebilir. Fakat günümüz teknolojisiyle NSA'in bütün dünyayı her türlü imkânla dinleyerek elde ettiği verilerle kişilere özel profiller çıkardığı bir gerçektir. NSA'in bunca veriyi işlemek için kullandığı devasa işlemci gücünü anlamak açısından bu işlemcilerin soğutulması için üç adet nükleer santralin enerjisinin doğrudan bu soğutma işlemine ayrıldığını söylemek yeterli olacaktır. Aynı şekilde NASA'da uzay istasyonları aracılığıyla gök cisimlerinin hareketlerini takip etmek ve çeşitli hesaplamalar yapmak için gereken işlemci gücünü elde edebilmek maksadıyla, gönüllülere çeşitli programlar yükletip bilgisayarlarının işlemci gücünü kullandığı bir proje yürütmüştür. Bütün bunlar göz önüne alındığında bitcoin ekosisteminde işlenen verinin NASA'dan mı NSA'den mi yoksa toplanan her türlü veri ile dünyanın yarınını tahminlemeye yönelik farklı bir projeden mi geldiğini söylemek imkânsızdır. Fakat harcanan bunca işlemci gücünün sadece rastsal bir kod üretmek için harcanması da pek mantığa uygun gelmemektedir. Özetle bitcoinin, bitcoin ağına dâhil olanların işlemci güçlerinden faydalanılarak devasa veriler işlemek için kullanılan bir proje olabileceği de ihtimal dâhilindedir. Hangi ihtimalin gerçekleşeceği bilinmez fakat bitcoin veya kriptopara sistemlerinin çökmesi durumunda gelmiş geçmiş en büyük ekonomik etkiye sahip siber saldırı olarak tarihe geçeceği kesindir.

1.9 BİLGİSAYAR VİRÜSÜ

Bilgisayar virüsleri bilgisayarları ve bilişim sistemlerini bozmaya, sekteye uğratmaya veya bu sistemler üzerinden bilgi toplamaya yönelik genel olarak kullanıcının haberi olmadan kullanıcı zararına işlemler yapan programlar şeklinde tanımlanabilir. Morris virüsü, duqu, tinba, red octobor virüsü, Shamoon virüsü ve Stuxnet virüsü en meşhur örneklerindendir. Çoğu, endüstriyel casusluk yoluyla bilgi çalmak için veya devletler için önem arz eden kritik alt yapı sistemlerini işlemez hale getirmek için kullanılmıştır. Tür olarak ta kendi içlerinde Ağ Virüsleri, Boot Sector (Ön Yükleme Sektörü) virüsleri, dosya virüsleri, karma virüsler, makro virüsleri gibi türleri mevcuttur.

1.10 ANTİ VİRÜS

Anti virüsler kullanıcıların bilgisayar virüslerinden etkilenmelerini engellemek amacıyla yazılmış programlardır. Anti virüsler bünyelerinde bir çeşit virüs listesi barındırır. Bu listede daha önceden tespit edilmiş kötücül kodlar yani virüs kodları örnekleri bulunur. Anti virüs programı bünyesindeki bu kodları kurulu olduğu ortamlardaki dosyaların kodları ile karşılaştırır ve eşleşme bulursa virüsü tespit etmiş olur. Sonrasında kullanıcıya uyarı verip dosyayı karantinaya alır ya da siler.

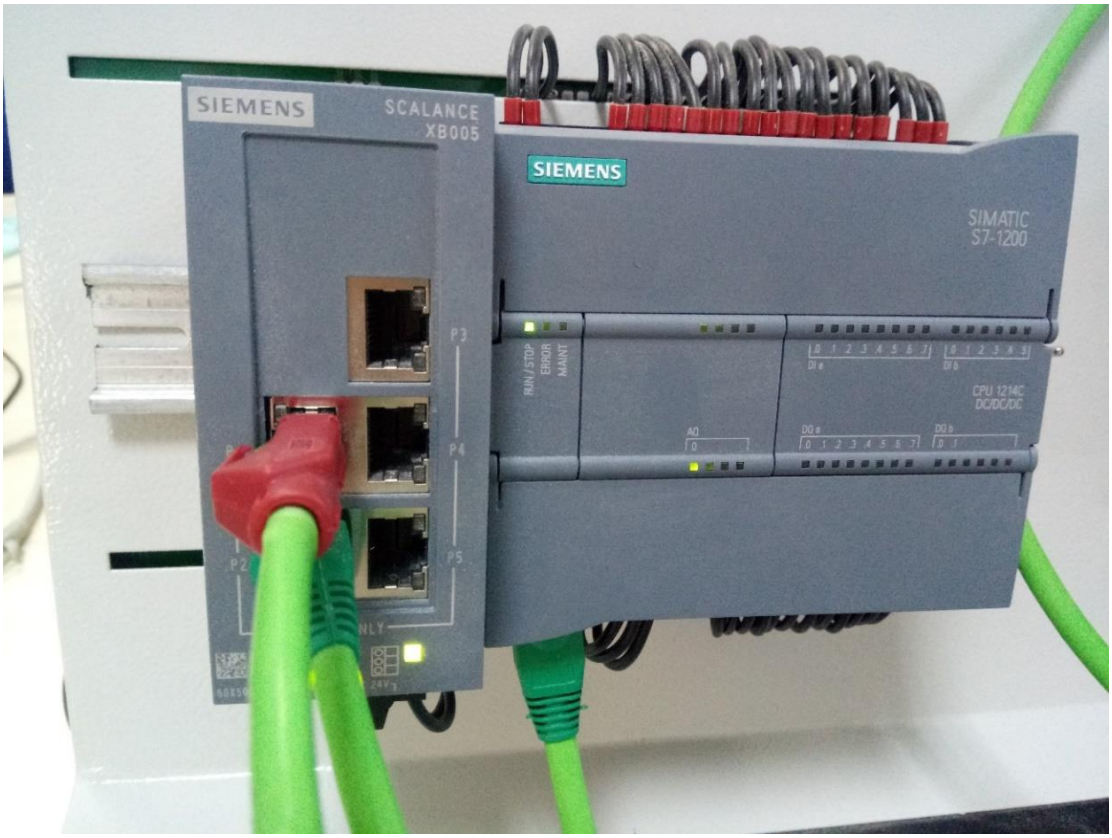
1.11 FİREWALL (GÜVENLİK DUVARI)

Güvenlik duvarının donanım olarak veya yazılım olarak bulunan çeşitleri mevcuttur. Güvenlik duvarları bilgisayar ağlarını dışarıdan gelebilecek tehditlere karşı korumak amacıyla tasarlanmış programlardır. Daha açık ifade etmek gerekirse bilgisayara virüs bulaşmasını veya izinsiz erişimleri engellemek amacıyla çalışmaktadır. Genel olarak ağ iletişimini izler ve tehlike algıladığında önlem alıp uyarı verirler. Örnek vermek gerekirse sertifikası geçerli olmayan bir internet sitesine girmeye çalıştığınızda güvenlik duvarı sizi uyaracaktır ve bağlantıyı açmayacaktır. Siber saldırılar güvenlik duvarı ve antivürüs üreten firmalar açısından hem tehdittir hem de fırsattır. Siber saldırılar arttıkça, bu tür önleme yazılımlarına olan talep te artmaktadır. Fakat bu tür yazılımlar atlatıldığında ise firmalara olan güven ve dolayısıyla talep azalmaktadır. Veya başka bir açıdan siber saldırılar arttıkça güvenlik çözümü üreten firmalar yeni teknikler geliştirmek için harcamalarını arttırmaktadırlar.

1.12 PROGRAMMBLE LOGIC CONTROLLER (PLC)

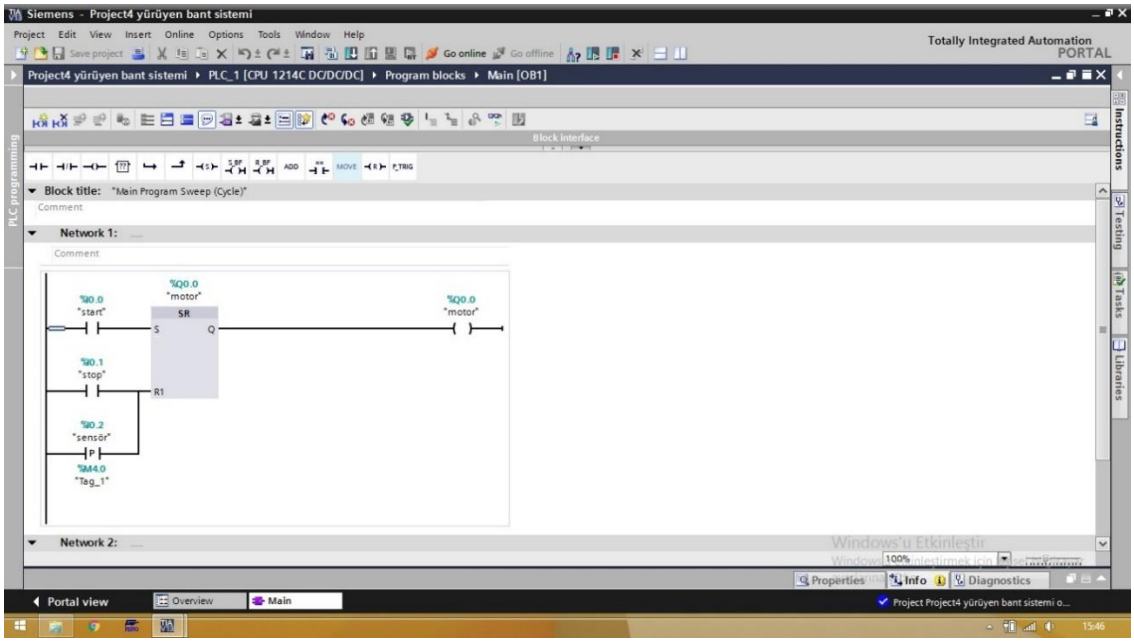
Programmble Logic Controller (PLC) algılayıcılardan (sensör) aldığı bilgiyi kendisine yüklenen programda verilen komutlar doğrultusunda işleyen ve çıkış elemanlarına aktaran mikroişlemci tabanlı bir çeşit bilgisayardır. Fabrikalarda bulunan üretim hatlarını oluşturan robot, taşıyıcı bant, pnömatik ekipman vb. gibi makinelerin elektromekanik kontrolü için kullanılır. Üzerlerinde tıpkı bilgisayarlar gibi giriş ve çıkış bağlantıları bulunur. Bu sayede çeşitli algılayıcılardan gelen verinin okunması,

oluşturulan program senaryosuna göre çeşitli çıkış birimlerinin (motor sürücüler, solenoid valfler v.b. gibi eyleyiciler) kontrolü ve diğer giriş/çıkış ve izleme (SCADA) birimleri ile haberleşmenin sağlanmasında görev alır.



Şekil 9: Örnek bir PLC Siemens'in S7-1200 Modeli
Kaynak: Görsel BŞEÜ-EDMEM PLC kursundan

Şekil 9'da görmüş olduğunuz Siemens'in S7-1200 modeli bir PLC'dir. Ethernet kabloları ile biden fazla PLC aynı anda birbiri ile haberleşerek de kullanılabilmektedir.



Şekil 10: Örnek bir PLC programı
Kaynak: Görsel BŞEÜ-EDMEM PLC kursundan

Şekil 10'da ise Siemens marka PLC'leri programlamak için kullanılan TİA Portal programı görülmektedir. TİA portal ortamında programlama şematik olarak ilerlemektedir. Programın işleyişinde gerekli olan parçalar görselde görülen şemaya eklenir, programa tanıtılarak spesifik özellikleri belirlenir ve çeşitli ayarları yapılır. Örneğin eklediğimiz parça bir sensör olsun. Şemada sensörü bir start stop işlemi için anahtara da bağlayabiliriz veya sayım işlemi için bir sayaca da bağlayabiliriz. Bu üretim kurgusuna göre değişebilir daha pek çok farklı değişken ve bağlantı kurulabilir. Görselde yazdığım program band üzerinde algılayıcıların bir nesne tespit etmesi durumunda bandı durduran bir programdır. Örneğin bandın üzerine bir koli konulduğunda koli algılayıcı hizasına geldiğinde bant durur. PLC'ler bant motorlarını kontrol etmekte kullanılabildikleri gibi nükleer santrallerde santrifüj motorlarını kontrol etmek için de kullanılabilmektedirler.

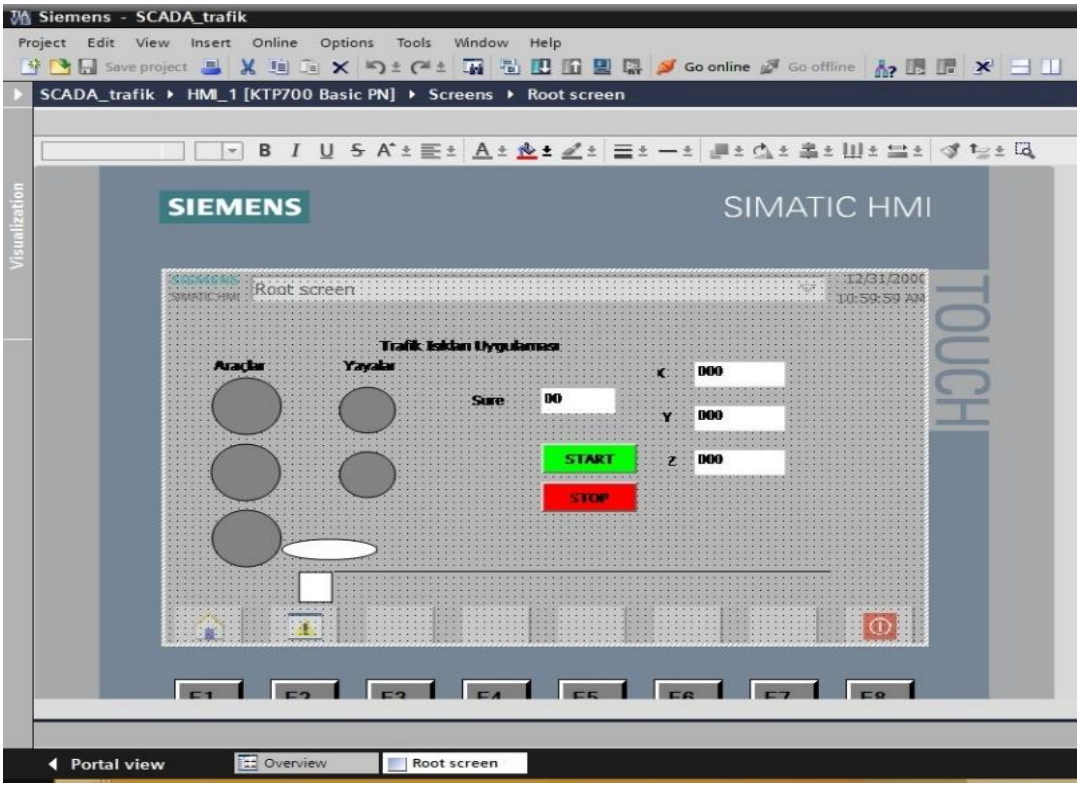
1.13 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

Endüstriyel kontrol sistemleri içinde programlanabilir mantıksal denetleyiciler(PLC), endüstriyel uygulamaların her alanında kullanılmaktadır. Denetimli kontrol ve veri toplama (Supervisory control and data acquisition – SCADA) ise geniş

alanda çalışan cihazların bir merkezden izlenmesi, veri toplanması, kaydedilmesi ve önceden belirlenmiş iş akışlarının takibine yarayan bilgisayar tabanlı sistemlerdir.

Şekil 11: Siemens marka bir SCADA operatör paneli
Kaynak: Görsel BŞEÜ-EDMEM SCADA kursundan

Şekil 11'de görülen SCADA kontrol panelinde programlamış olduğum bir KTL (Kathodische Tauchlackierung – katodik daldırma boyama) işlemini yürüten program görülmektedir. Dokunmatik panel sayesinde süreçlere panel üzerinden müdahale edilebilmektedir. SCADA sistemleri raylı ulaşım sistemlerinden tutun da PLC ler ile birlikte nükleer santrallere kadar endüstride geniş bir yelpazede süreç takip ve kontrolleri amacıyla kullanılmaktadır. SCADA'nın amacı önceden programlanıp hazırlanan standart uygulamaları HMI(Human Machine Interface) insan makine arayüzü ekranından müdahale ederek programlama ile tekrar uğraşmaya gerek kalmadan gerçekleştirmektir. Veya bir diğer açıdan programlama bilgisi olmayan çalışanların da oluşturulan menüler aracılığıyla işleri yürütebilmesini sağlamakta faydalarından biridir. SCADA ve PLC sistemleri üretimde etkinlik açısından hemen her alanda sıkça kullanıldığı için, son zamanlarda siber saldırıların da gözde hedefleri haline gelmişlerdir.

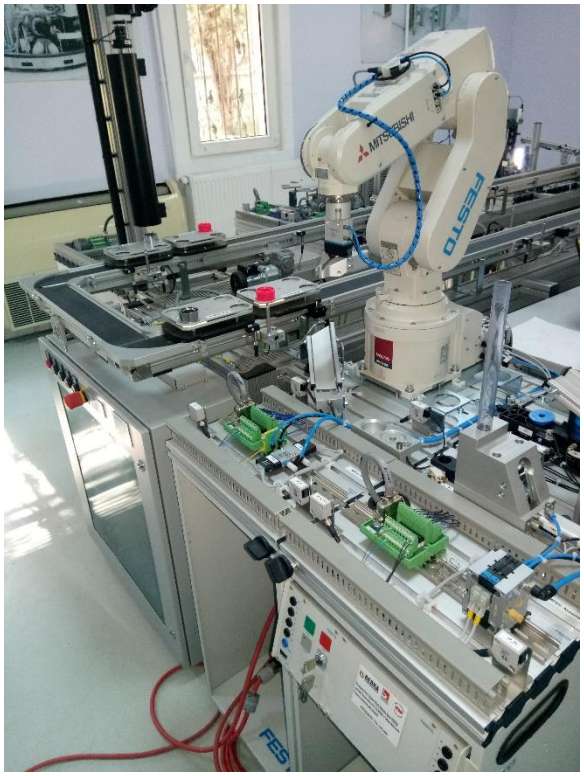


Şekil 12: Örnek bir SCADA programı
Kaynak: Görsel BŞEÜ-EDMEM SCADA kursundan

Şekil 12'de görmüş olduğunuz Siemens Tia Portal ortamında hazırlamış olduğum bir trafik ışığı uygulaması görülmektedir. Programdaki şekilleri ve etiketleri tamamen kendimiz amaca göre hazırlıyoruz. Gerekli değişken ve bağıntıları girdikten sonra PLC ve SCADA arasında haberleşen sistem verileri SCADA kontrol panelinde bizim girmiş olduğumuz akışa göre görselleştirmektedir. Sonrasında programlama aşamasında yerleştirdiğimiz butonlar ve menüler üzerinden tekrar programlama gerekmeden işler yürütülebilmektedir.

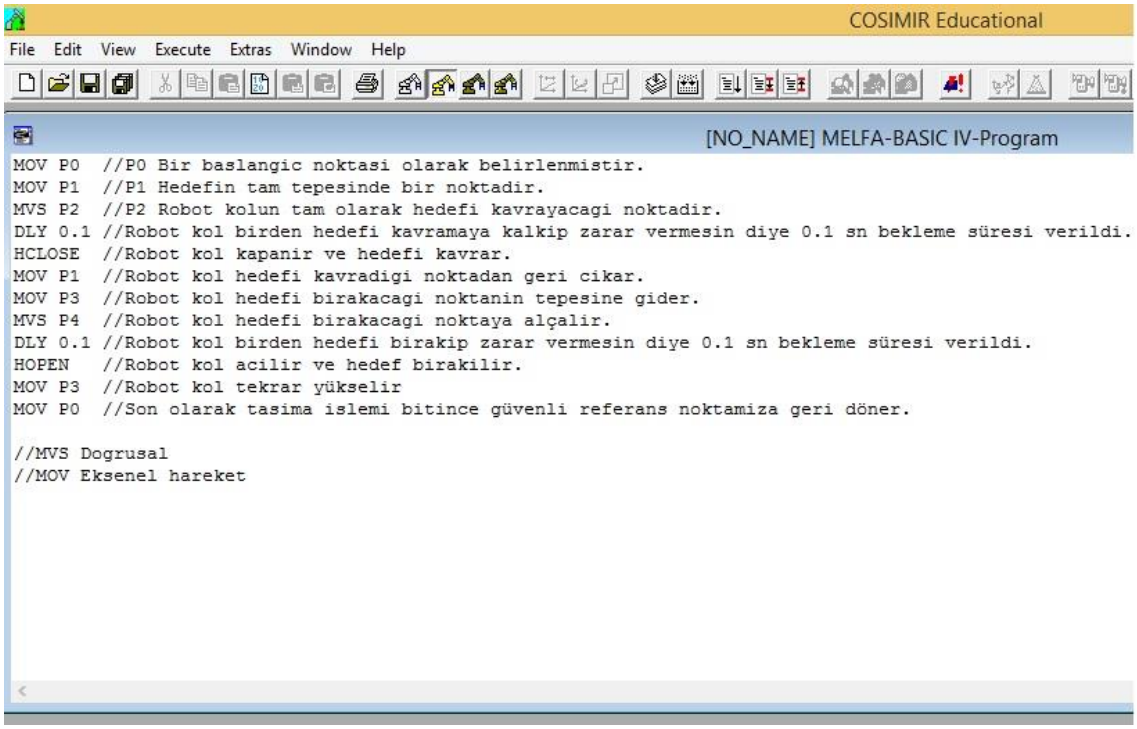
1.14 ENDÜSTRİYEL ROBOTLAR

Endüstride montaj hattından, kaynak yapımına kadar geniş yelpazede kullanılan, günümüzde tıp ve başka alanlarda da kullanılmaya başlayan otomatik kontrollü, yeniden programlanabilir makinelerdir. Üç ve daha fazla eksene sahip modelleri de mevcuttur.



Şekil 13: Örnek bir endüstriyel robot
Kaynak: Görsel BŞEÜ-EDMEM Robotik kursundan

Şekil 13'de görmüş olduğunuz Mitshubishi'nin Festo model bir endüstriyel robotudur. Robot kolun ucuna takılan araca göre farklı işlerde kullanılabilmektedir. Robotlar, genel kanının aksine insan uzuvları gibi esnek hareket etmemektedirler. Benzer esnekliği kazandırabilmek için programlama aşamasında detaylı bir çalışma yapmak gerekmektedir. Robotlar milimetrik olarak hareketleri uyguladıkları için tanımlanan işi yaparken hareket ettikleri eksen ve koordinatların belirlenmesini kolaylaştırmak amacıyla kontrol paneli ile koordinatlar programa girilmektedir. Ayarlanan değerler ve açı ve hız eğer uygun değilse tanımlanan işi yaparken sorunlar yaşanabilmektedir. Örneğin bir parça ürünü bir montaj hattından başka bir montaj hattına taşımak gibi temel bir işlevin yapılmasında dahi kavrama noktası ve açısı iyi ayarlanmalıdır. Fakat bir kez gerekli ayarlamalar yapıldığında durdur komutu gelene dek durmaksızın hatasız olarak çalışabilmektedirler.



Şekil 14: Örnek bir robot programı
Kaynak: Görsel BŞEÜ-EDMEM Robotik kursundan

Şekil 14'de ise Cosimir ortamında yazmış olduğum Melfa Basic IV programı, bir noktadan başka bir noktaya parça taşıyan bir robot programı görülmektedir. Programın aşamaları "//" kaçış karakteri kullanılarak görselde adım adım anlatılmıştır.

1.14.1 İlk Robot Cinayeti

Endüstride kullanılan robotlar kullanım amacına göre çeşitli boyutlarda olabilmektedir. Görsellerde gördüğünüz ufak robotlardan araba fabrikalarında montaj hatlarında kullanılan devasa robotlara kadar farklı çeşitleri mevcuttur.

Robotlar yukarıda görüldüğü gibi sabit bir program ile programlanabildiği gibi yapay zekâ ile üretim etkinliğine yönelik programlanmış robotlarda mevcuttur. İlk robot cinayeti de 1981'de Kawasaki fabrikasında yapay zekâ ile kontrol edilen bir robot tarafından işlenmiştir. Robotu yöneten yapay zekâ, bir çalışanı hatalı bir şekilde üretim engeli olarak algıladığı için, çalışanı yok etmesi gerektiğini düşünüp devasa kollarıyla tutup yakınındaki öğütme makinesine atmıştır (Goodman, 2016:460).

1.15 3D VE 4D YAZICILAR

Üç boyutlu (3D) yazıcılar Filament denilen termo plastik maddeler kullanarak, sanal ortamda tasarlanan 3 boyutlu nesneleri, gerçek hayata 3 boyutlu olarak aktaran mekanizmalardır. Filament, makaraya sarılı halde bulunan 3D yazıcıda belirli bir ısı ve düzende eritilerek baskı yapılmasını sağlayan maddedir, deyim yerindeyse 3D yazıcıların kartuşudur. Filament olarak genelde termo plastik kullanılsa da, amaca göre farklı maddelerde kullanılabilmektedir. 3D yazıcı teknolojisi ile telefon kabı, biblolar, oyuncaklar, aksesuarlar, çeşitli eğitim materyalleri, mutfak eşyaları, robot parçaları, birebir maketler ve hatta 3D yazıcıyı oluşturan parçaların bir kısmı ve daha pek çok şey basılabilmektedir. Dört boyutlu (4D) yazıcılar ise programlanabilir malzeme denilen, nanoteknoloji ürünü maddeler kullanarak, hareketli veya çevre şartlarına tepki veren cisimler basan yazıcılardır. 4D teknolojisi henüz deneysel aşamada olmakla birlikte gelecek vadetmektedir.

Bu teknolojilerin üretim yöntemi olarak değerlendirilip ekonomik sonuçlarının tartışılması gerekmektedir. Ekonomi tarihine baktığımızda geçmişte, üretim yöntemleri ve ekonomik modeller kültürel kavramlara paralel olarak karşıtlarını oluşturdular ve üretim yapıları ve modeller hem kültürü etkilediler hem de kültürden etkilendiler. Taylorizm, gelişen teknoloji ve değişen kültür ile birlikte yerini Taylorizm ’in eksiklerini gideren Fordizm’e bıraktı. Fordizm’in eksiklerine karşı olarak Postfordizm ortaya çıktı. Ancak Postfordizmin de eksikleri vardı. Postfordizm’de 20. yy. da yerini Keynesyen iktisada bıraktı. Keynesyen İktisat ’ta kendi postunu yarattı ve Postkeynesyenler ortaya çıktı. Bu devinim sürekli devam etti ama egemen gruplar bunun farkına vardılar. Ve kapitalizm sürekli yeni kalmayı amaç edinerek varlığını günümüze kadar sürdürebildi. Reklamlar, farklılaştırılmış ürünler, kişiye özel ürünler ve bu ürünleri seri bir şekilde üretebilecek sistemler ile kapitalizm hep yeni kaldı ya da kendini öyle gösterdi. 3D ve 4D teknolojilerinin gelişmesi ile gelinen noktada her bireyin kendine özel üretim tesisi olacağı bir üretim kültürüne doğru ilerlemekteyiz. Üretim yöntemlerinin değişmesi geçmişte olduğu gibi kültürü etkileyecek ve birikim yöntemleri de değişecektir.

Günümüzde 3D yazıcıların büyük çoğunluğu, başka bir 3D yazıcı üretmek için gereken parçaların %50’sini üretebilmektedir ve bu oran hızla artmaktadır. Pazar araştırmaları 2018’de üç boyutlu yazıcı pazarının %500 büyüyerek 16 milyar dolara

ulaşacağını söylemektedir. Gartner Group, 3D baskı teknolojisinin 2018'den itibaren her yıl en az 100 milyar dolar fikri mülkiyet kaybına yol açacağını tahmin etmektedir (Goodman, 2016, s:448,449). ABD ordusu 2017'de bir denizaltı aracını ve güçlü bir bomba fırlatıcısını 3D basım tekniğiyle üretmiştir. Hackerlar internet üzerinden çaldıkları planlarla dünyanın herhangi bir yerinde kontrol dışı büyük zararlar verecek silahlar üretebilir (Eczacıbaşı, 2018, s:175). Nitekim bu tür olaylar da yaşanmıştır. *HaveBlue adlı bir şirkette mühendis olarak çalışan Michael Guslick, AR-15 tarzı yarı-otomatik silaha ait yapım şemalarını internetten indirdi ve 3D yazıcıdan çıkardığı detaylı şablonlarla, silahı 3D yazıcıda üretmeyi başardı. Guslick, 3D yazıcı ile kendisinin ürettiği 22 kalibrelik silahla 200 el ateş ettiğini açıkladı(https://shiftdelete.net/3d-yazicisiyla-yari-otomatik-tufek-uretti-39105, 23.7.2018).*

Görüldüğü üzere 3D ve 4D gibi teknolojiler geliştikçe, bilgi gelecekte sermayenin yerini alacaktır. Dolayısıyla bilginin ve bilgi güvenliğinin de önemi giderek artacaktır. Gerek fikri mülkiyet ihlalleri açısından olsun, gerekse savunma ekonomisi ve silah sanayi açısından olsun yukarıdaki örnekte olduğu gibi, siber saldırılarla bu tür tasarım bilgilerinin çalınması ciddi ekonomik etkilere, taraflara bağlı olmakla birlikte, negatif veya pozitif dışsallıklara yol açacaktır.

1.16 KÜRESEL İZLEME SİSTEMLERİ VE ASİMETRİK BİLGİ

Bilgi: öğrenme, araştırma veya gözlem yolu ile elde edilen gerçektir(http://sozluk.gov.tr).

Simetrik her iki tarafta da aynı olan, asimetrik ise iki tarafta farklı olan anlamına gelmektedir. Asimetrik bilgi ise tarafların herhangi bir konuda eşit bilgiye sahip olmaması durumunu ifade eder. Ekonomi literatürü açısından bu bilgi ekonomik gerçeklikler hakkında, piyasa gerçekleri hakkında bir tarafın diğerinden daha fazla bilgi sahibi olmasını ifade eder. Bu bilgi eşitsizliği, daha çok bilgi sahibi olan tarafa haksız avantajlar sağlamaktadır. Asimetrik bilginin bu tür haksız avantajlar sağlaması ahlaki tehlike, ters seçim ve asil-vekil sorunlarını doğurmaktadır.

Ahlaki Tehlike Ve Asil vekil sorunu

Başkasını temsilen iş yapan kurum, kuruluş veya kişilerin temsil ettikleri merciden habersiz olarak onların zararına olacak şekilde hareket etmesi veya yaptıkları işlerde gereken özeni göstermemesi. İşçilerin kaytarmasından tutun da, 2008 krizine neden olan bankaların yöneticilerine kadar çeşitli örnekler verilebilir. Asil vekil sorununun bir diğer örneği de geçmişte ülkemizde yaşanan "banka hortumlama" diye tabir edilen olaylardır. Banka yöneticileri çeşitli tekniklerle bankalardaki mevduatları boşaltmışlardır.

Ters Seçim Sorunu

Tam bilgiye sahip olmayan tarafın ekonomik açıdan kendi avantajına olmayan seçimler yapmasını ifade eder. Bu soruna genellikle sigorta piyasası ve bankaların kredi politikaları örnek gösterilir. Bankalar verdikleri kredileri kredi alanların kârlı veya kârsız yatırımlara mı harcayacaklarını, yüksek riskli veya risksiz yatırımlara mı harcayacaklarını bilemezler. Bu yüzden faiz oranlarını yüksek tutarlar. Bunun sonucunda yüksek kredi faizleri kredi alanları, kredi faizini karşılayıp kâr edebilmek için yüksek riskli yatırımlara yöneltir. Yüksek riskli yatırımların başarısız olması sonucunda banka kredilerini ödeyemezler. Bu durumun yarattığı bir diğer etki de gerçekten risksiz yatırımlarla para kazanıp kredisini ödemeyi düşünen müşterilerin yüksek faiz oranlarından dolayı kredi çekememesidir. Burada bilgi asimetrisinden kaynaklanan bir ters seçim söz konusudur. Bankalar kredi talep eden müşterilerin yatırımlarının risklilik düzeyini bilememektedirler. Zaten günümüzde de bu tür sorunları ortadan kaldırmak için pek çok çalışma ve iş modeli geliştirilmiştir. Günümüzde bankalar çoğu kredi talebinin nerede kullanılacağına dair bilgi talep etmektedirler. Bu doğrultuda ev kredisi, tüketici kredisi, yatırım kredisi gibi çeşitlendirmelere gitmişlerdir. Bankaların bu yöndeki bir diğer çözümü de kişisel kredi notu veri tabanları oluşturmak olmuştur. Bugün bankalarla muhatap olmamış olsanız bile bankaların çeşitli yöntemlerle sizin hakkınızda elde ettikleri verilerden yola çıkarak oluşturdukları kredi notlarınız bulunmaktadır. Bankalar üzerinden anlattığımız bütün bu işleyiş sigorta şirketleri açısından da aynı şekilde işlemektedir. Ve günümüz imkânları düşünüldüğünde hakkınızdaki bütün bu bilgileri siber ortam sayesinde elde etmekte ve paraya dönüştürmektedirler. İş durumunuzdaki gelişmeler, gelir durumunuzdaki gelişmeler, harcama eğilimleriniz, tasarruf eğilimleriniz

tüketim harcamalarınızı belirleyen ilgi alanlarınız bütün bu bilgiler ve daha fazlası paraya dönüştürülebilecek değerli bilgilerdir.

Limon Piyasalar ve Kalite Belirsizliği

Akerlofun ikinci el araba pazarından verdiği örneği uyarlarsak şöyle bir durumu tarif etmektedir:

İkinci el arabaların satıldığı bir araba pazarı düşünelim. Bu araba pazarında 500 adet iyi ve 500 adet te kötü, yani limon diye tabir ettiği arabalar olsun. Arabası iyi durumda olan satıcılar arabalarını 20.000 ile 24.000 arasında bir fiyata satmak istiyorlar. Arabası kötü durumda olan satıcılar da 10.000 ile 12.000 arasında bir fiyata satmak istiyorlar. Bu durumda ortalama araba fiyatı 15.000 ile 18.000 arasında olacaktır. Limon arabaların sahipleri için 15.000 oldukça iyi bir fiyat olduğundan, arabalarını bu fiyatlara satmak konusunda bir sorun yaşamayacaklardır. Fakat iyi araba sahipleri için durum böyle değildir. Arabası iyi durumda olanlar, 20.000 den aşağı bir fiyata satmayı düşünmedikleri için, arabalarını satmaktan vazgeçip, arabalarını bu araba pazarından çekeceklerdir. Geriye sadece kötü arabalar kalacaktır ve bir süre sonra bu araba pazarından kimse araba almamaya başlayacaktır ve araba pazarı piyasası çökecektir.

Akerlof'un ekonomik etkilerini ortaya koyduğu asimetrik bilgi kavramı bilişim çağını yaşayan günümüz dünyasında, eskisinden çok daha önemli hale gelmiştir. Devletler küresel izleme sistemlerine ve değerli bilgi üreten büyük veri yatırımlarına oldukça önem vermektedirler. NSA ve ECHELON gibi izleme sistemleri dünyada artık hemen hemen her ülkenin geliştirmeye çalıştığı, sahip olmaya çalıştığı siber istihbarat mekanizmalarıdır ve hali hazırda pek çok ülkenin mevcut yapılanmaları bulunmaktadır. Bu ülkelerin birimleri, elde ettikleri bilgileri değerledikten sonra veya tasnifledikten sonra sadece askeri amaçlarla değil ekonomik amaçlarla da kullanmaktadırlar. NSA bazen diğer kurumlar, uzmanlar ve hatta ulusal çıkarlar doğrultusunda özel sektörle de bilgi paylaşımı içerisindedir. Örneğin NSA ve ABD Savunma Bakanlığı, saldırı imzalarını bir grup kritik savunma yüklenicisi ile paylaşmak için ortak çalışmıştır. Ayrıca NSA 2010'da gerçekleşen saldırılardan sonra Google'a ve 2012'deki hizmet dışı bırakma saldırılarından sonra finans endüstrisine teknik yardım sunmayı kabul etmiştir (Singer & Friedman, 2015, s:269).

Bu tür dinleme mekanizmalarının ne şekilde asimetrik bilgi ve limon piyasa modeline neden olduğunu anlatmak için AB, ABD ve İngiltere arasında krize neden olmuş, Avrupa Parlamentosu kayıtlarına geçmiş bir olayın haberi aktarılmıştır:

ABD telefonları dinleyip ihale casusluğu yapıyormuş

ABD'nin komünizme karşı kurduğu Echelon adlı gizli teşkilatın, telefonları dinleyerek İngilizce konuşan ülkelere ihale kazandırdığı ortaya çıktı. Raytheon Corporation ve Boeing gibi şirketlerin bu yolla büyük paralar kazandığı iddia edilirken Fransa ABD ve İngiltere'yi dava ediyor. ABD'nin 1947 yılında Komünist Blok'a karşı kurulan ve hala resmen açıklanmayan Echelon adlı gizli örgütlenmeyi, İngilizce konuşulan ülkelerin yararına sanayi casusluğunda kullandığı ortaya çıktı. Fransa ABD ve İngiltere'ye dava açmaya hazırlanırken, Almanya ve İtalya parlamentoları da soruşturma başlattı.

İddiaya göre, ABD önderliğinde İngiltere, Kanada, Avustralya ve Yeni Zelanda Echelon casusluk sistemini kendi amaçlarına kullanmaya başladı. Casusluk ağı, Avrupa hükümet ve şirketlerinin telefon, faks, elektronik posta gibi verilerine girerek bu bilgileri ticari amaçlarla İngilizce konuşulan ülkelerin şirketlerine ulaştırdı. Bu iddia da ortalığı karıştırmaya yetti. ABD'nin liderliğinde 5 İngilizce konuşulan ülkenin kendi çıkarları için kullanmaya başladığı Echelon sisteminin Soğuk Savaş döneminde, 1947 yılında, Komünist Blok'a karşı kurulduğu belirtiliyor. Ancak batı Avrupa ülkeleri, Ulusal Güvenlik Ajansı'na (NSA) bağlı olan Echelon'un, Avrupa ülkelerindeki ticari sırları Amerikan işadamlarına iletmekte kullandığını öne sürüyorlar.

PARLAMENTONUN RAPORU

Avrupa Parlamentosu'nun 1997 yılında hazırladığı rapor, 22 Şubat 2000 tarihinde AP Sivil Özgürlükler Komitesi'nde ele alınacak. Raporda, Amerikan NSA tarafından bazı bilgiler ele geçirildikten sonra Amerikan şirketlerinin Avrupa firmalarındaki bazı ihaleleri kazandığına ilişkin suçlamaların yer aldığı belirtiliyor. AP raporunda, Amerikan NSA'in 1995 yılında elektronik devi Fransız Thomson CSF şirketinin, 800 milyon sterlinlik (720 trilyon), Brezilya yağmur ormanları için uydu izleme sistemi ihalesiyle ilgili olarak Brezilyalı yetkililerle görüşmelerini ele geçirdiği ve bunları Thomson CSF'in Amerikalı rakibi Raytheon Corporation'a verdiği kaydediliyor. Raytheon Corporation daha sonra bu ihaleyi kazanmıştı.

KONGRE SORUŞTURMA AÇTI

Ayrıca 1993 yılında Fransa önderliğinde Avrupa konsorsiyumu Airbus'un, Suudi Arabistan Havayolları ve Suudi yetkililerle görüşmelerinin de yine NSA tarafından ele geçirilerek Amerikan Boeing şirketine ilettiği ve Boeing'in de 3.7 milyar sterlin (3.3 katrilyon) değerindeki ihaleyi kazandığı belirtiliyor. ABD Kongresi'nin de Echelon sistemiyle ilgili soruşturma başlattığı ve federal yetkilileri dinleyeceği belirtiliyor. Avrupa Parlamentosu'nun raporundan önce 1996 yılında Yeni Zelanda'da yayınlanan bir kitapta Echelon'dan bahsedilmesine karşılık, ne ABD ne

de İngiltere Echelon'un varlığını onaylamıştı (http://www.hurriyet.com.tr/dunya/abd-telefonlari-dinleyip-ihale-casuslugu-yapiyormus-39133560 , 07.07.2019).

Örnekte de görüldüğü gibi NSA gibi küresel izleme sistemleri haksız rekabete neden olmaktadır. Bir diğer önemli etkileri de önceleri NSA'in resmi internet sitesinde yazan fakat şuanda kaldırılmış olan *"Hiçbir ülkenin bilimde ABD'den daha ileride olmamasını sağlamak"* misyonlarının bir sonucu olarak diğer ülkelerden hatta kendi ülkelerindeki özel firmalardan dâhi, işlerine yarayacak know how bilgilerini, tasarımları ve ARGE bilgisini çalmalarıdır. Bu tür bilgiler yıllar süren araştırmaların, deneyimlerin, harcanan yığınla para ve emeğin ürünüdür. Bu izleme sistemlerinin bu tür bilgileri genel olarak siber ortam aracılığı ile elde etmesi açısında bu tür izleme sistemlerini aralıksız olarak süren siber saldırılar olarak düşünebiliriz. Ve görüldüğü üzere bu saldırılar sonucunda el değiştiren bilginin ekonomik maliyetini hesaplamak neredeyse imkânsızdır. Yukarıdaki haberde gördüğünüz üzere küresel izleme sistemleri ile elde edilen bilgilerin ihale öncesinde kendi firmalarına verilmesi sonucu ortaya çıkan zararın boyutlarını hesaplamak oldukça güçtür. Bir diğer açıdan kendi firmaları için de kârlı bir duruma yol açmıştır. Genel anlamda bakıldığında ise ihaleyi kazanmaması gereken firmalar kazandığı için de kaynakların etkin kullanılamamasına neden olmuştur. Havayolu ihalesini Boeing değilde Airbus kazanmış olsaydı hava yolları ulaştırma sektöründe etkinlik söz konusu olacaktı. Belki de bugün aldığınız uçak bileti biraz daha ucuz olacaktı. Bunlar muhtemel etkiler fakat net etki olarak bakarsak havayolu ihalesinden kazanılan para Fransa'ya veya AB'ye değil de İngiltere'ye gitmiştir. Buda en sade haliyle 3.7 milyar sterlinlik bir siber saldırı ekonomik etkisidir. Ve son olarak bunlar sadece bilinen örneklerdir. Bu güne kadar kaç ihaleye müdahale edildi, kaç tasarım çalındı, bu çalınan bilgiler ne şekilde kullanıldı, daha kim bilir ne ekonomik etkileri olduğu bilinmemektedir.

1.17 NSA (ULUSAL GÜVENLİK AJANSI)

4.11.1952 tarihinde ABD'de kurulmuştur. NSA'in asıl kuruluş amacı hiçbir ülkenin bilimde ABD'den daha ileride olmamasını sağlamaktır. 1990'lı yılların başlarında 96 ülkede yılda 3.000.000 görüşmeyi dinleyebilecek kapasiteye gelmiştir. Sovyetler Birliği'nin yıkılmasında önemli rol oynadığı ileri sürülmektedir. Çalışan sayısı net olarak açıklanmasa ve çok gizli tutulsa da 30.000 civarı olabileceği tahmin edilmektedir.

NSA Ülke dışı Sinyal İstihbaratı Direktörlüğü ve ABD bilişim sistemlerini koruyan, Bilgi Güvencesi Direktörlüğü olmak üzere iki temel birimden oluşur.

NSA'in Stratejisi:

- *Küresel kriptolojide en üstün olma*
- *Güvenli milli güvenlik sistemleri tesis etme*
- *İnsanları, sistemleri, sensörleri ve bilgileri küresel çapta birbirine bağlama*
- *Hükümet, akademi, endüstri ve yabancı ortaklarla ilişkileri geliştirme* (Çifci, 2017, s:42).

Bir e-mail ve dosya şifreleme sistemi olan PGP (Pretty Good Privacy) şifreleme sistemini geliştiren Phil Zimmermann'la çalışmış olan Smari McCarthy, NSA'in programlarını ve ABD hükümetinin tüm güvenlik bütçesini tüm yönleriyle incelemiştir. İncelemeleri sonucunda dünyadaki tüm internet kullanıcılarının gözetlenmesinin, NSA'e günlük 13 sente mal olduğunu hesaplamıştır (Bartlett, 2016, s:109).

1.18 ÇİN NSA'İ

Pekin'de kurulu olan Halkın Kurtuluşu Ordusu (PLA)'nın genelkurmaya bağlı üçüncü bölümü, sinyal istihbaratı ve kod kırma çalışmalarıyla NSA'e benzemektedir. Söylendiğine göre bölümün 130.000'e yakın çalışanı bulunmaktadır. PLA'nın 61539 Birimi olarak ta bilinen Pekin Kuzey Bilgisayar Merkezi'nin ise Çin'in Siber Komutanlığı olduğu söylenmektedir. Bu birimin ülke genelinde konuşlu en az on iki ilave eğitim tesisi ve bilgisayar ağı savunma, saldırı ve istismar sistemleri tasarlama ile ilgili en az on, alt bölümü vardır. PLA'nın 3. Ordu 2. Büroya bağlı 61398 Birimi olarak ta bilinen Şangal Grubu ise ABD hakkında siyasi, ekonomik ve askeri bilgiler toplamakla görevlendirilmiştir (Singer & Friedman, 2015, s:192). Bu bahsi geçen kurum ve kuruluşlar sadece kaynaklarda bahsedilenlerdir. Çin'in siber gücünü oluşturan başka kurumların da olduğu düşünülmektedir fakat bu tür oluşumlar devletler tarafından mümkün mertebe gizli tutulmaktadır.

1.19 RUS NSA'İ

Rusya 2000 yılı sonrasında milli güvenlik politikasını yeniden ele almış ve bilgi harekâtı stratejileri üzerine odaklanmıştır (Çifci, 2017, s:98). Moskova'da FAPSI(Devlet iletişim ve Bilişim Federal Komisyonu) isimli NSA benzeri bir kuruluşları vardır. Sovyetler çöktükten sonra, 2003 yılında FAPSI'nin ismi Özel İletişim ve Bilişim Servisi olarak değiştirilmiştir. Güney Rusya'da Voronezh kentinde, FAPSI dünyanın en büyük hacker okulunu işletmektedir (Clarke & Knake, 2011, s:37). Ayrıca Rusya çıkardığı 152 numaralı Federal Kanun'la, kişisel verilerle ilgili belirtilen çok kısıtlı durumlar haricinde, Rusya'daki internet servis sağlayıcıların yabancı bir ülkenin yetkili birimlerine bilgi vermesi yasaklanmıştır (Çifci, 2017, s:98). Bu sayede siber ortamda gerçekleştirdiği vekâlet savaşları yasal olarak sorgulanamaz hale gelmiştir.

1.20 ECHELON (BEŞ GÖZ)

Avustralya, Kanada, Yeni Zelanda, Birleşik Krallık, Amerika Birleşik Devletleri arasında ilk olarak Birleşik Krallık ve Amerika Birleşik Devletleri tarafından Mart 1946'da imzalanan UKUSA antlaşması ile elektronik istihbarat alanında işbirliği yapılması kapsamında kurulan küresel izleme sistemidir.

1.21 PROMİS (PROSECUTOR'S MANAGEMENT INFORMATİON SYSTEM)

PROMIS yazılımı 1980'lerde ABD'de bulanan küçük çaplı bir yazılım şirketi olan Inslaw şirketinde Bill Hamilton isimli yazılımcı tarafından geliştirilmiştir. PROMIS'in açılımı Savcılık Bilgi Yönetim Sistemi'dir. Geliştirilme amacı adalet sisteminde artan dosya yükünü hafifletmek ve soruşturması yürütülen davalar arasında bağlantı olup olmadığını tespit ederek soruşturmalara yardımcı olmaktı. Fakat program şirketin bilgisi dışında CIA ve MOSSAD tarafından çalınarak suçluların veya bu istihbarat örgütlerinin hedeflerinin izini sürmek gibi çeşitli amaçlarla kullanılmaya başlanmıştı. Bill Hamilton programının çalındığını bir MOSSAD ajanının teknik bir sorunu çözmek için şirketle irtibata geçmesiyle öğrendi. Hamilton ABD adalet sistemiyle iletişime geçip dava açtı fakat programın çalınmasından dolayı şirketi çoktan iflas etmişti (Gökdemir, 2013, s. 25).

CIA ve MOSSAD, PROMIS yazılımını modernize edip başka ülkelerin istihbarat servislerine de satmaya başladılar. Programa yerleştirdikleri arka kapı sayesinde programı kullanan ülkelerin istihbarat servislerinin de içine girmiş oldular. Programı satın alan ülkeler arasında Türkiye, Kıbrıs, Pakistan, Suriye, Kuveyt ve Irak'ta vardı. İsrail Irak'a yerleştirdiği bu casus yazılım sayesinde tespit ettiği, Irak'a silah satan birçok kişiyi MOSSAD ajanları aracılığıyla infaz etmiştir (Gökdemir, 2013, s:27).

PROMIS yazılımı elinde bulunan veri tabanındaki çeşitli verileri sınıflandırarak bu veriler arasında bağıntılar kurmak yoluyla çalışmaktadır. Örnek vermek gerekirse; aranan bir suçlunun bağlantılı olduğu kişiler, dava dosyalarında işlenmektedir. Ve bu kişilerin bağlantılı olduğu kişiler de. PROMIS yazılımı, adalet bakanlığı veri tabanı bankaların veri tabanları, elektrik, su, doğalgaz gibi altyapı hizmetlerinin veri tabanlarını ve daha pek çok veri tabanını bünyesinde barındırır. Bu veri tabanlarında aranan kişi ve etkileşimde olduğunu tespit ettiği kişilerin, banka hesaplarında bir anormallik tespit ederse program bunu değerlendirir, bulundukları adreslerde bir anormallik tespit ederse bunu değerlendirir. Örneğin aranan kişinin bağlantılı olduğunu tespit ettiği birisinin ev adresinde fazladan su tüketimi olmuşsa, program bunu o evde fazladan birisi var diye yorumlar ve kullanıcıya uyarı verir. CIA ve MOSSAD'ın PROMIS üzerinde yaptıkları değişikliklerden sonra program aynı zamanda kullandığı veya kendisine yüklenen her veri tabanını tek bir veri tabanında birleştirmeye başlamıştır. Dolayısıyla CIA ve MOSSAD programa ekledikleri arka kapı ve elde edilen veri tabanlarını tek bir yerde birleştirme özelliği ile PROMIS'i kullanan her ülkede atılan her adımdan haberdar olmuşlardır. PROMIS'in algoritması hakkında herhangi bir bilgi bulunamamakla birlikte, sınıflandırma açısından finanstan tutunda tıbbi tanılamaya kadar, pek çok alanda kullanılan Naive Bayes öğrenen algoritmasını temel alan bir çeşit sınıflandırma algoritması kullanılmış olabilir.

1.22 SAVAŞ EKONOMİSİ VE SİBER SAVAŞ

NSA, PROMIS, ECHELON, Çin'in NSA'i ve Rusya'nın NSA'i gibi dünyada daha pek çok devletin siber komutanlıkları, siber istihbarat birimleri, hacker orduları ve siber aleme yönelik savaş birimleri bulunmaktadır. Fakat bu tür birimler ve ülkelerin askeri birimleri ve bahsi geçen siber birimleri mümkün mertebe dünyadan gizlenmektedir. Elimizde yer alan istatistikler üzerinden ülkelerin küresel ateş gücü

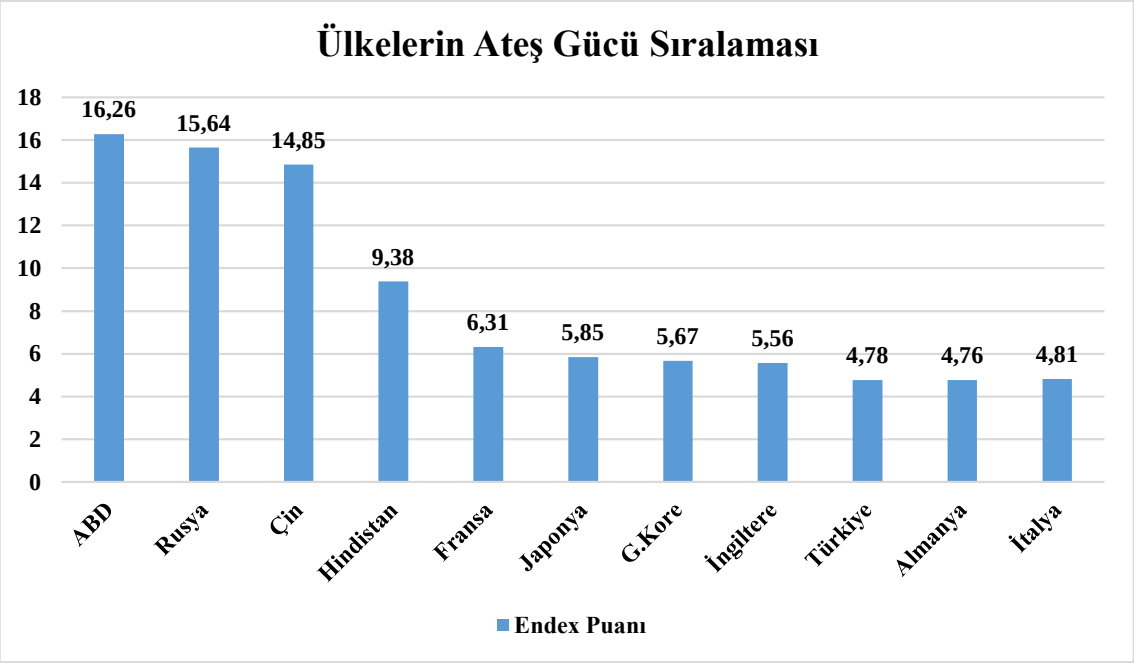
endeks puanlarını ve küresel siber gücü endeks puanlarını karşılaştırdığımızda sıralamanın birbirine paralel gitmediğini görmekteyiz. Bu duruma sebep olan etmenlerin başında da bazı ülkelerin siyasi olarak sorun yaşamadıkları bir coğrafyada bulunması dolayısıyla çok fazla askeri güce ihtiyaç duymaması gibi özel durumlar yer almaktadır.

Grafik 14'de globalfirepower'ın 55'in üzerinde bireysel faktörü kullanarak hazırlamış olduğu ülkelerin küresel ateş gücü index puanlarının grafiği görülmektedir.

Endex puanları:

- Toplam nüfus
- Savunma bütçesi
- Mevcut insan gücü
- Toplam askeri personel
- Aktif personel
- Toplam hava gücü
- Savaş tankları
- Zırhlı Savaş Aracı
- Toplam deniz varlıkları

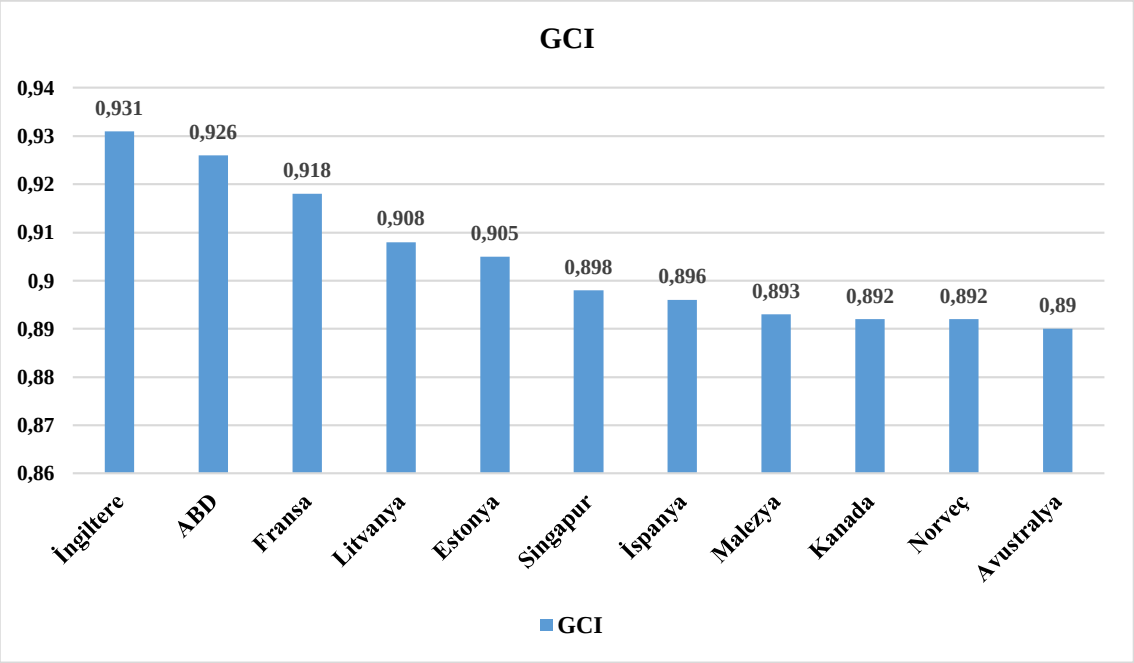
Gibi kriterler dikkate alınarak hesaplanmıştır.



Grafik 14:Ülkelerin Ateş Gücü Sıralaması

Kaynak: Global Fire Power 2019, (https://www.globalfirepower.com/countries-listing.asp , 20.06.2019)

***** Grafiğin daha iyi anlaşılabilmesi içi gerçek puanlar 1'e oranlanarak yeniden hesaplanmıştır



Grafik 15: Ülkelerin Küresel Siber Güvenlik Endex Puanları
Kaynak: International Telecommunication Union(ITU), Global Cybersecurity Index 2018 raporundaki veriler kullanılarak oluşturulmuştur.

Grafik 14 ve grafik 15'de görüldüğü üzere ülkelerin siber güvenlik sıralamaları ve askeri sıralamaları farklı olabilmektedir.

Ülkelerin GCI index puanları hesaplanırken de tablo 4'te gösterilen göstergeler ve ağırlık puanları kullanılmıştır. Tabloda dikkat çektiği üzere puan verilen hususlar teknik önlem, yasal önlem, strateji, kapasite geliştirme ve işbirliği ana başlıkları altında toplanmıştır.

Tablo 4:GCI Puanlamasında Kullanılan Göstergeler Ve Ağırlıkları

NO	GÖSTERGELER	AĞIRLIK
1.	Yasal önlemler	0.2
1.1	Siber Suçlar Mevzuatı	0.079
1.2	Siber Güvenlik Yönetmeliği	0.079
1.3	Spam mevzuatının sınırlandırılması / engellenmesi	0.042
2.	Teknik önlemler	0.2
2.1.	Ulusal, Hükümet, Sektörel CERT / CIRT / CSIRT	0.065
2.2.	Organizasyonlar İçin Siber Güvenlik Standartları Uygulama Çerçevesi	0.035
2.3.	Standardizasyon Kurumu	0.030
2.4.	İstenmeyen postalara yönelik teknik mekanizmalar ve yetenekler	0.024
2.5.	Siber güvenlik amaçlı bulut bilişim kullanılması	0.019
2.6.	Çevrimiçi Çocuk Koruma mekanizmaları	0.027
3.	Organizasyonel Tedbirler	0.2
3.1.	Strateji	0.092
3.2.	Sorumlu Ajans	0.063

3.3.	Siber Güvenlik Metrikleri	0.045
4.	Kapasite geliştirme	0.2
4.1.	Halkın Bilgilendirilmesi Kampanyaları	0.036
4.2.	Siber Güvenlik Standartları ve Profesyoneller İçin Sertifikalandırma	0.027
4.3.	Siber Güvenlik Mesleki Eğitim Kursları	0.032
4.4.	Milli Eğitim Programları ve Akademik Müfredatlar	0.032
4.5.	Siber Güvenlik Araştırma ve Geliştirme Programları	0.026
4.6.	Teşvik Mekanizmaları	0.024
4.7.	Ülke İçi Geliştirilen Siber Güvenlik Endüstrisi	0.023
5.	İşbirliği	0.2
5.1.	Çift taraflı anlaşmalar	0.038
5.2.	Çok Taraflı Anlaşmalar	0.038
5.3.	Uluslararası forum / derneklerin katılımı	0.036
5.4.	Kamu-özel ortaklık	0.034
5.5.	Kurumlararası / kurum içi ortaklıklar	0.026
5.6	Siber güvenlik en iyi uygulamaları	0.028
	Toplam	**1**

Kaynak: International Telecommunication Union(ITU), Global Cybersecurity Index 2018

Siber güvenlik gücünü geliştirmek açısından bu tür tablolar oldukça önem arz etmektedirler. Ülkelerin siber güvenlik strateji eylem planı hazırlarken bu tür başlıkların siber saldırı, siber savaş, siber güvenlik ve ulusal güvenlik açısından kendi ülkelerinde ne derece önem arz ettiğini iyi analiz etmelidirler.

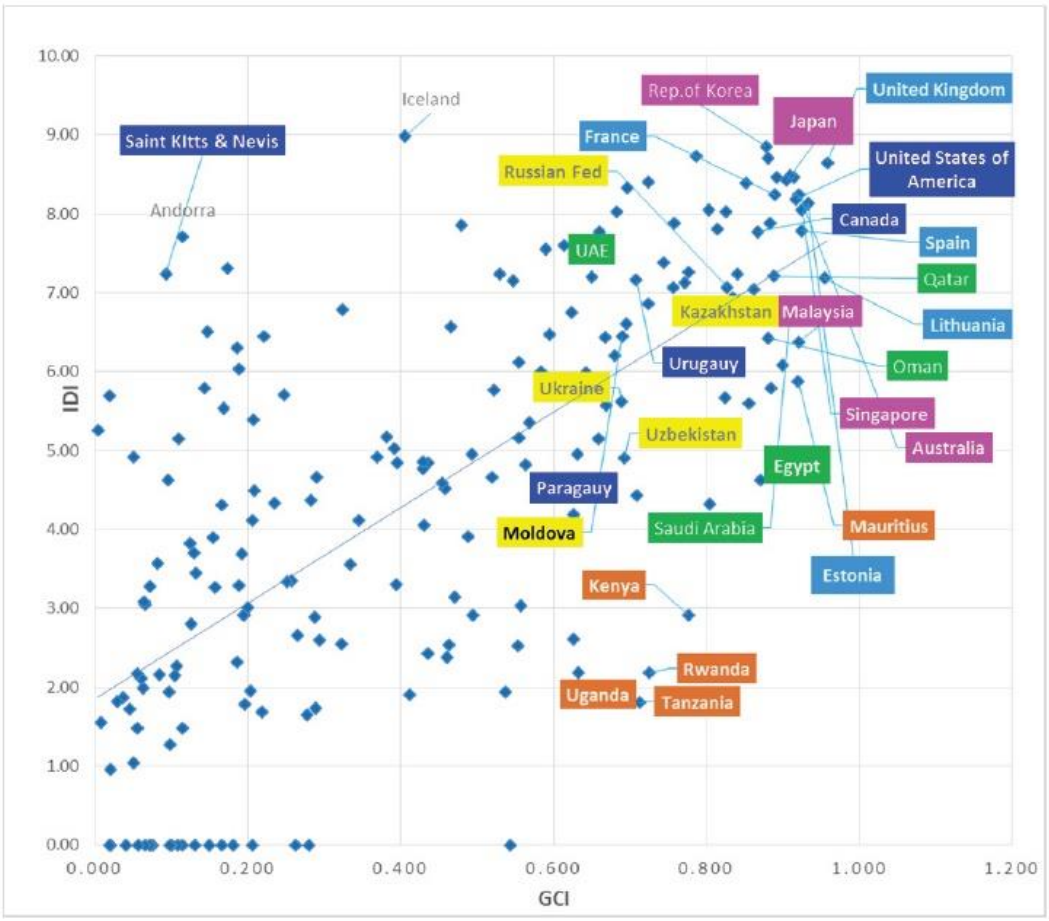
Tablo 5: Ülkelerin GCI ve GPI Sıralamaları

ÜLKE	GCI	GPI
İngiltere	1	8
ABD	2	1
Fransa	3	5
Litvanya	4	81
Estonya	5	112
Singapur	6	59
İspanya	7	20
Malezya	8	41
Kanada	9	21
Norveç	9	36
Avustralya	10	19

Kaynak: International Telecommunication Union ve Global Fire Power'dan alınan verilerle oluşturulmuştur

Tablo 5'te görüldüğü üzere küresel siber güvenlik sıralamasında ilk sırada yer alan İngiltere küresel ateş gücü sıralamasında 8. sırada yer alırken, ABD'nin küresel siber

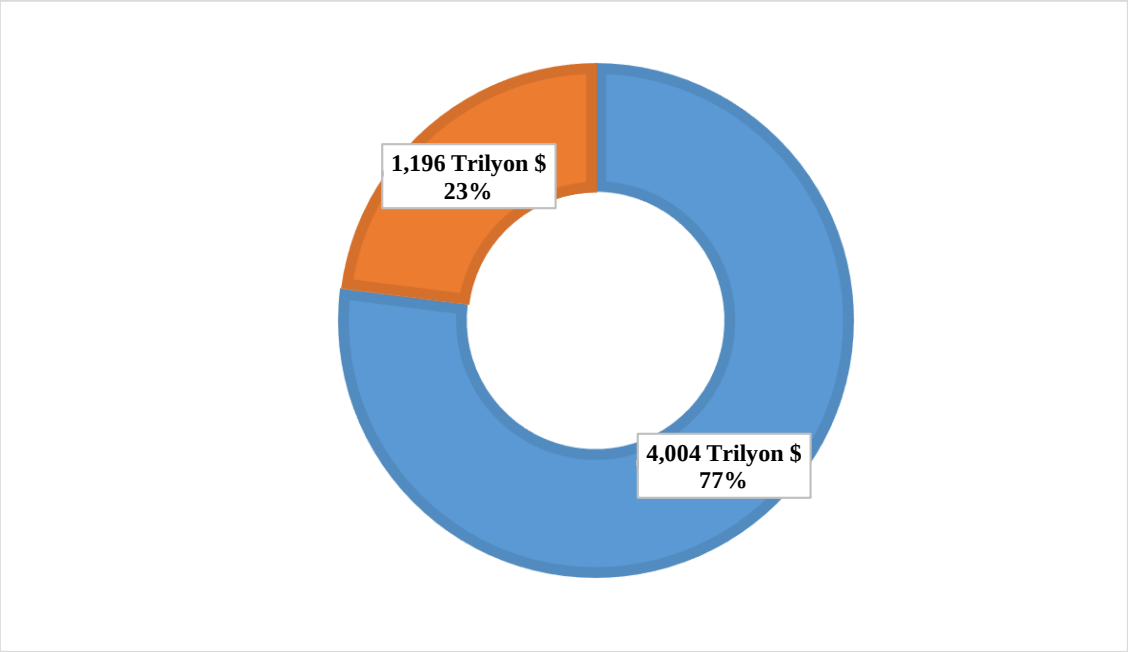
güvenlik ve ateş gücü sıralaması arasında aşırı bir farklılık gözükmemektedir. Tablo 5'te dikkat çeken ülkelerin başında Estonya gelmektedir. Aslında işin iç yüzünü bildiğimizde bu sıralama farkı çokta anormal değildir. Estonya Siber güvenlik endeksinde 5. sırada yer almaktadır ki bu Estonya büyüklüğünde bir ülke için ciddi bir başarıdır. Fakat bu başarının arkasında saldırı örneklerinde göreceğimiz üzere geçmişte yaşamış oldukları siber saldırılardan çıkardıkları dersler vardır. Burada da siber saldırıların yapıcı bir özelliğini görmek mümkündür. Estonya teknolojik entegrasyonu gelişmiş bir ülkedir ve böyle bir ülkede bu başarıyı sağlamalarından dolayı diğer devletlere bu konularda danışmanlık dahi yapabilecek bilgi birikimine sahip olduklarını söylemek mümkündür. Diğer bir örnek olan Litvanya ise ülkenin 2 milyonluk nüfusu ve siyasi olarak çok fazla sorun yaşamayan bir ülke olduğundan dolayı askeri güç olarak çok ön sıralarda görmemek normal olmakla beraber askeri yatırımlar yapmayan bu ülkenin siber güvenlik sıralamasında 4. sırada yer alması dikkat çekicidir. Buradan çıkaracağımız sonuç gerçek dünyanın savaş kuralları ile siber dünyanın savaş kuralları farklıdır. Gerçek dünyada sorun yaşamayan ülkeler dahi siber güvenliğe ciddi yatırımlar yapmaktadırlar. Çünkü siber ortam yapısı gereği sınır tanımamaktadır. Tablomuzda dikkat çeken bir diğer örnek ise Singapur'dur. Singapur siber güvenlik sıralamasında dünyada 6. sırada yer alırken askeri güç sıralamasında 59. sırada yer almaktadır. Singapur'un bu başarısının arkasında başarılı kalkınma ve eğitim stratejileri olduğunu söylemek zor değildir. Singapur yatırımlarını gelecek vadeden teknolojiler üzerinde yoğunlaştırmıştır.



Grafik 16: Bilişim Teknolojileri Gelişmişlik Endeksi (IDI) Ve Küresel Siber Güvenlik Endeksi (GCI)

Kaynak: International Telecommunication Union(ITU), Global Cybersecurity Index 2018

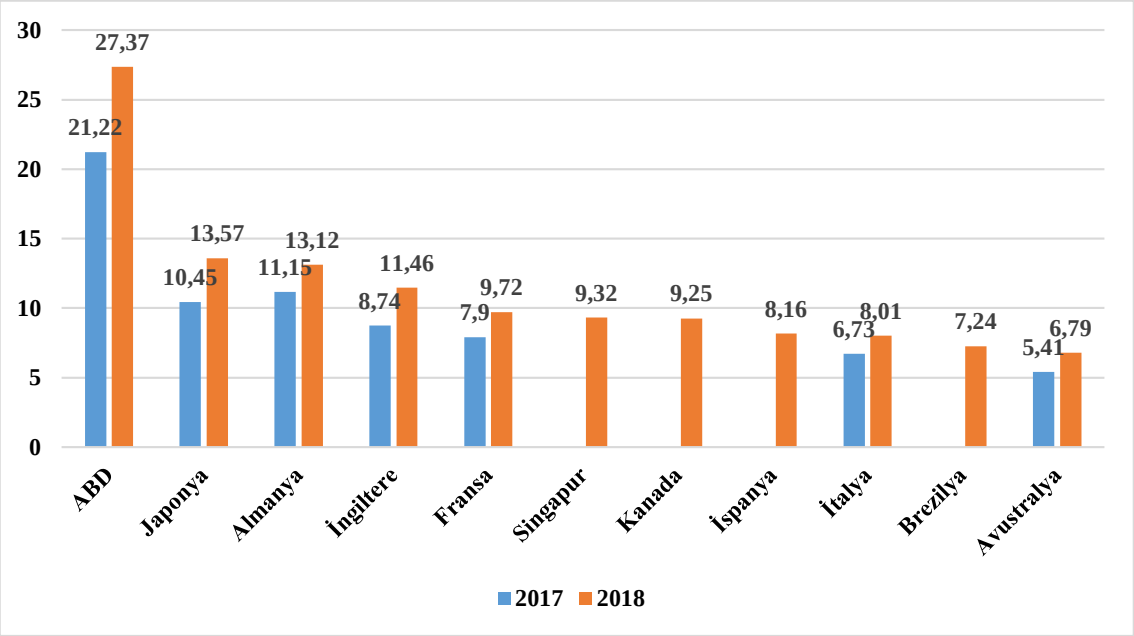
Bir diğer önemli konu da bilgi iletişim teknolojileri gelişmişlik endeksi(IDI) ile küresel siber güvenlik indeksi(GCI)'nin kıyaslanmasıdır. Grafik 16'da görüldüğü üzere bilişim teknolojileri gelişmişlik endeksi puanı ile küresel siber güvenlik endeksi puanlarının aynı olmadığı görülmektedir. Örneğin, İzlanda, GCI'da sadece 0.406 iken, IDI puanı 8.98'de en üst sırada yer almıştır. Andorra ve Saint Kitts ve Nevis, IDI'de yüksek, GCI'de ise çok düşük olmasına rağmen, bazı ülkeler her iki endekste de lider pozisyonlarını korumaktadırlar. Bilişim teknolojilerinin etkili ve esnek olması için, değişen ihtiyaçları yansıtacak şekilde siber güvenliğin uygulanması ve düzenli olarak güncellenmesi gerekir. Bilişim teknolojilerine paralel olarak geliştirilmeyen siber güvenlik ya gereksiz yere siber güvenlik yatırımları yapılmasına neden olacaktır, ya da gerektiği kadar siber güvenlik önlemi alınmamasından kaynaklı siber tehditler doğuracaktır.



Grafik 17: Doğrudan ve Dolaylı Siber Saldırıların Riske Attığı Değer Sonraki 5 yıl için tahminleme (Birikimli 2019-2023)

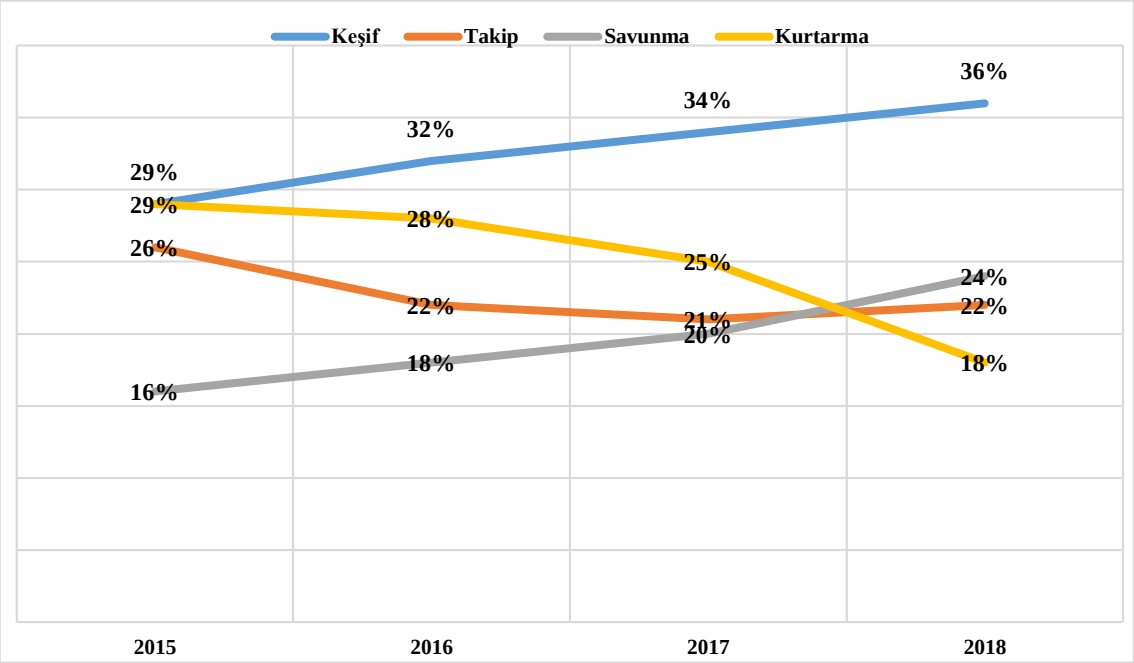
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu s:14, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50, 24.06.2019)

Ponemon Enstitüsünün, yapmış olduğu araştırmaya göre, sonraki 5 yıl için siber suçtan kaynaklı olarak risk altında olan değerin yaklaşık olarak 5.2 trilyon $ olduğu söylenmektedir. Bu riskin %77'si doğrudan siber saldırılardan kaynaklanırken %23'ü dolaylı siber saldırılardan kaynaklanmaktadır. Burada risk altında olan değerden kasıt alet, teçhizat, bilgisayar sistemleri olabildiği gibi siber saldırılardan kaynaklı olarak çalınan verilerin kötüye kullanımı da dâhil her çeşit risk altında olan değerdir.



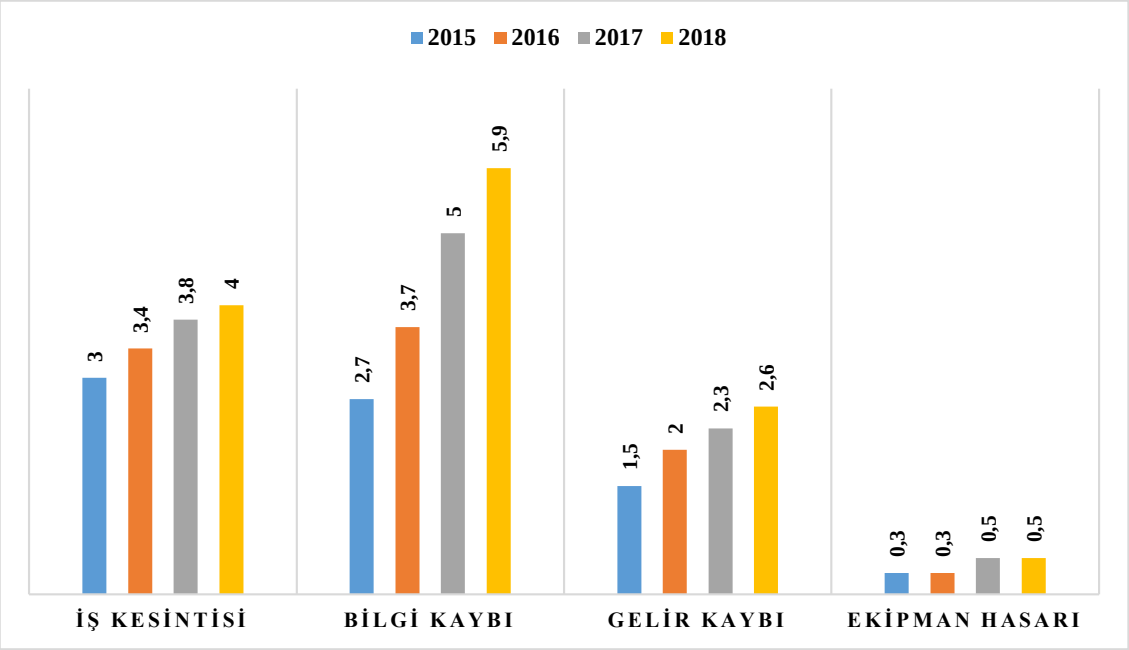
Grafik 18: Ülkelere Göre Yıllık Siber Suç Maliyeti (Milyon $)
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu

Grafik 18'de siber suçların ülkelere göre maliyetleri görülmektedir. Burada dikkat çeken husus küresel siber güvenlik indeksinde 2. sırada yer alan ABD'nin siber suçlara katlanılan maliyette 1. sırada yer almasıdır. Ve 2017 yılında katlandığı siber suç maliyeti ile 2018 yılında katlandığı siber suç maliyeti arasındaki farka baktığımızda ciddi bir yükseliş gözlenmektedir. Bu durumda etkili olan ülkenin büyüklüğü, ekonomik ve siyasi açıdan dikkat çekmesi, bilişim teknolojileri entegrasyonu gibi pek çok etmen vardır. Grafiğin geneline bakıldığında da siber suç maliyetleri yıllara göre hızla artış göstermektedir.



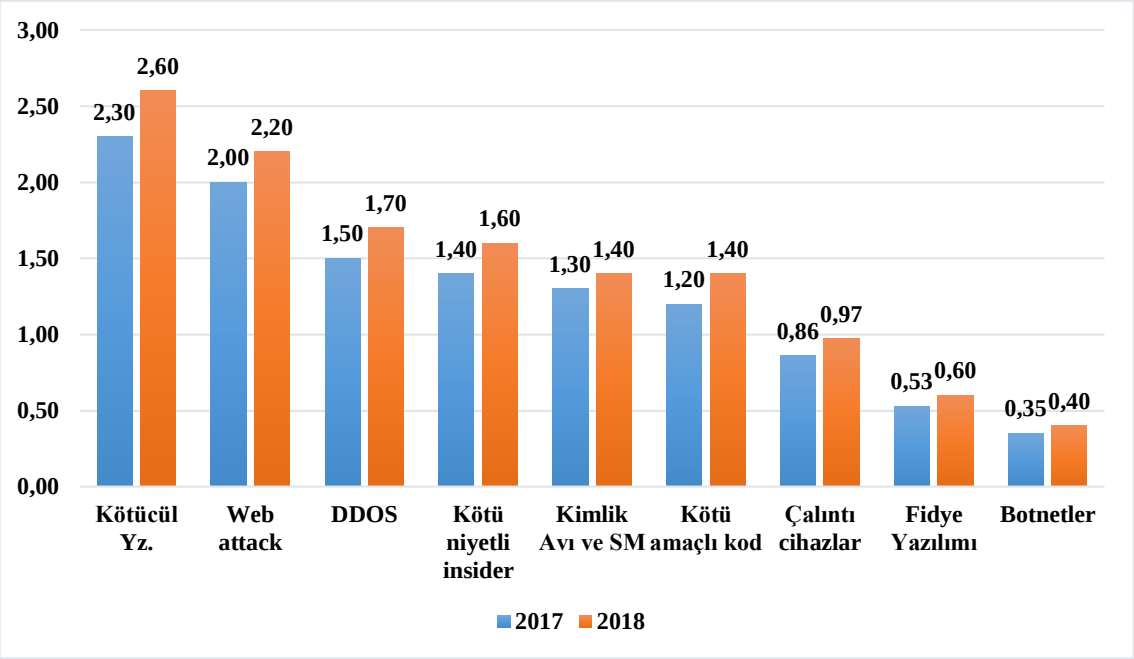
Grafik 19: İç Faaliyet Siber Güvenlik Harcamaları % Değişim
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu

Keşif faaliyetlerine yapılan harcama oranı giderek artmıştır. Buna karşın kurtarma faaliyetlerin yapılan harcamaların giderek azaldığı gözlenmektedir. Kurtarma faaliyetlerine yapılan harcamaların azalmasındaki en önemli etmenin, bulut bilişim teknolojilerinin gelişmesi ve kullanım alanlarının giderek yaygınlaşması olduğu düşünülmektedir. Savunma masrafları ise teknik personel işe alımı ve siber güvenliği sağlamak amacıyla yapılan harcamaların artması nedeniyle giderek artmaktadır.



Grafik 20: Saldırı Sonucu Ortalama Yıllık Siber Suç Maliyeti (milyon $)
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu

Grafik 20'de siber saldırı maliyetleri iş kesintisi, bilgi kaybı, gelir kaybı ve ekipman hasarı olmak üzere dört ana kategoride incelenmiştir. 2015-2018 yılları arasında tüm maliyet türlerinde artış görülmektedir. Siber suçların bu dört yıl için iş kesintisi toplam maliyeti 15.2 milyon $ bilgi kaybı olarak maliyeti 17.3 milyon $ gelir kaybı olarak maliyeti 8.4 milyon $ ekipman hasarı olarak maliyeti 1.6 milyon $'dır. En hızlı yükselen ve aynı zamanda en yüksek maliyet kategorisi bilgi kaybı kategorisidir. Bilgi kaybı maliyetlerindeki artıştan yola çıkarak gelecekte bulut bilişim sektörünün gelişeceği ön görülebilir.



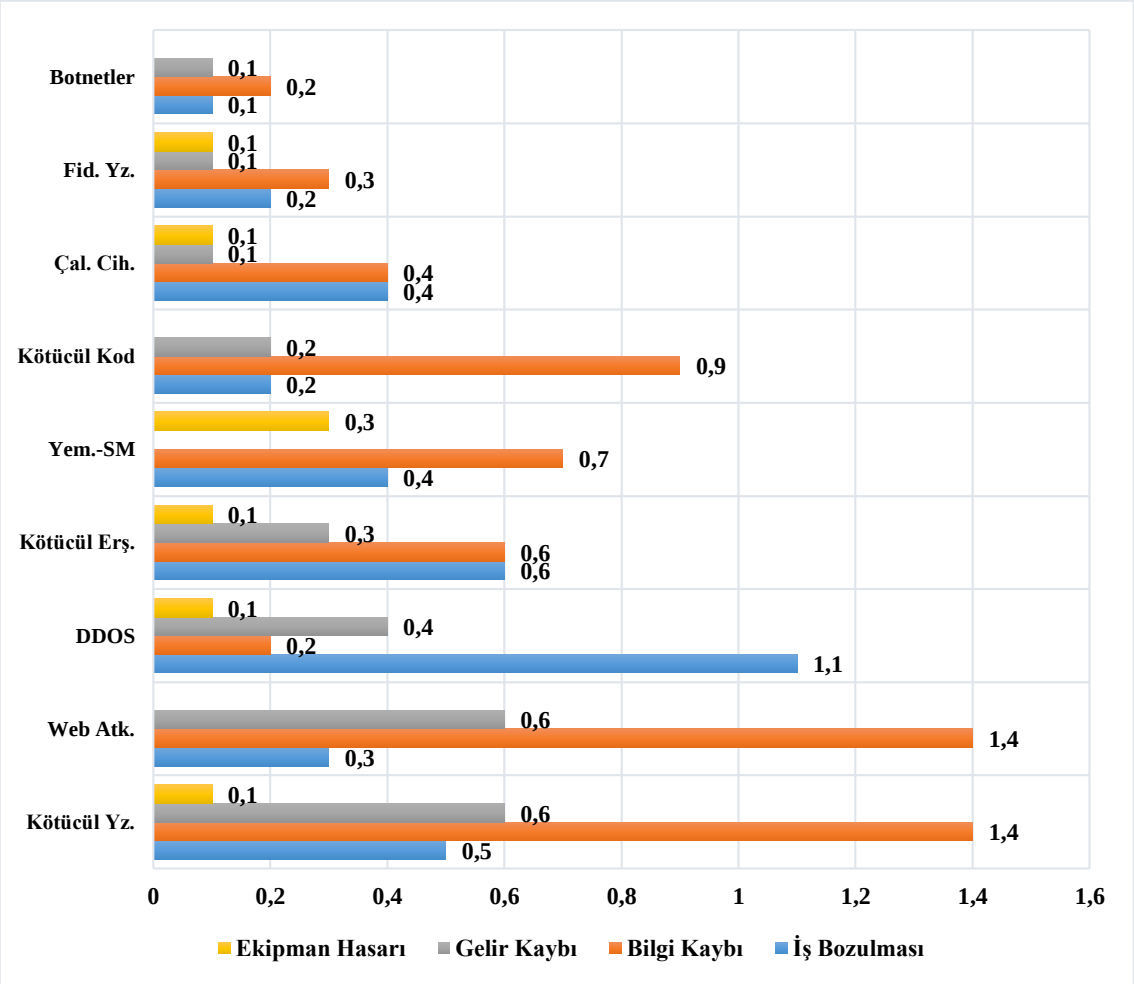
Grafik 21: Saldırı Türüne Göre Ortalama Yıllık Siber Suç Maliyeti (milyon $)
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu

***İnsider:** İçeriden kötü niyetli erişim

Grafik 21'de farklı saldırı türlerinin 2017 ve 2018 yılında verdikleri zararlar gösterilmiştir. En yüksek zararı Malware olarak tabir edilen kötücül yazılımlar vermişlerdir. Kötücül yazılımların zararı 2017'de 2.3 milyon dolarken 2018'de 2.6 milyon dolara çıkmıştır. Genel olarak tüm saldırı türlerinin maliyetlerinde artış görülmektedir. Saldırı türlerinin 2017 toplam maliyeti 11.44 milyon dolar, 2018 yılı toplam maliyeti ise 13 milyon dolar olmuştur. Saldırı hasarlarının yüzdelik olarak artışları ise şu şekildedir:

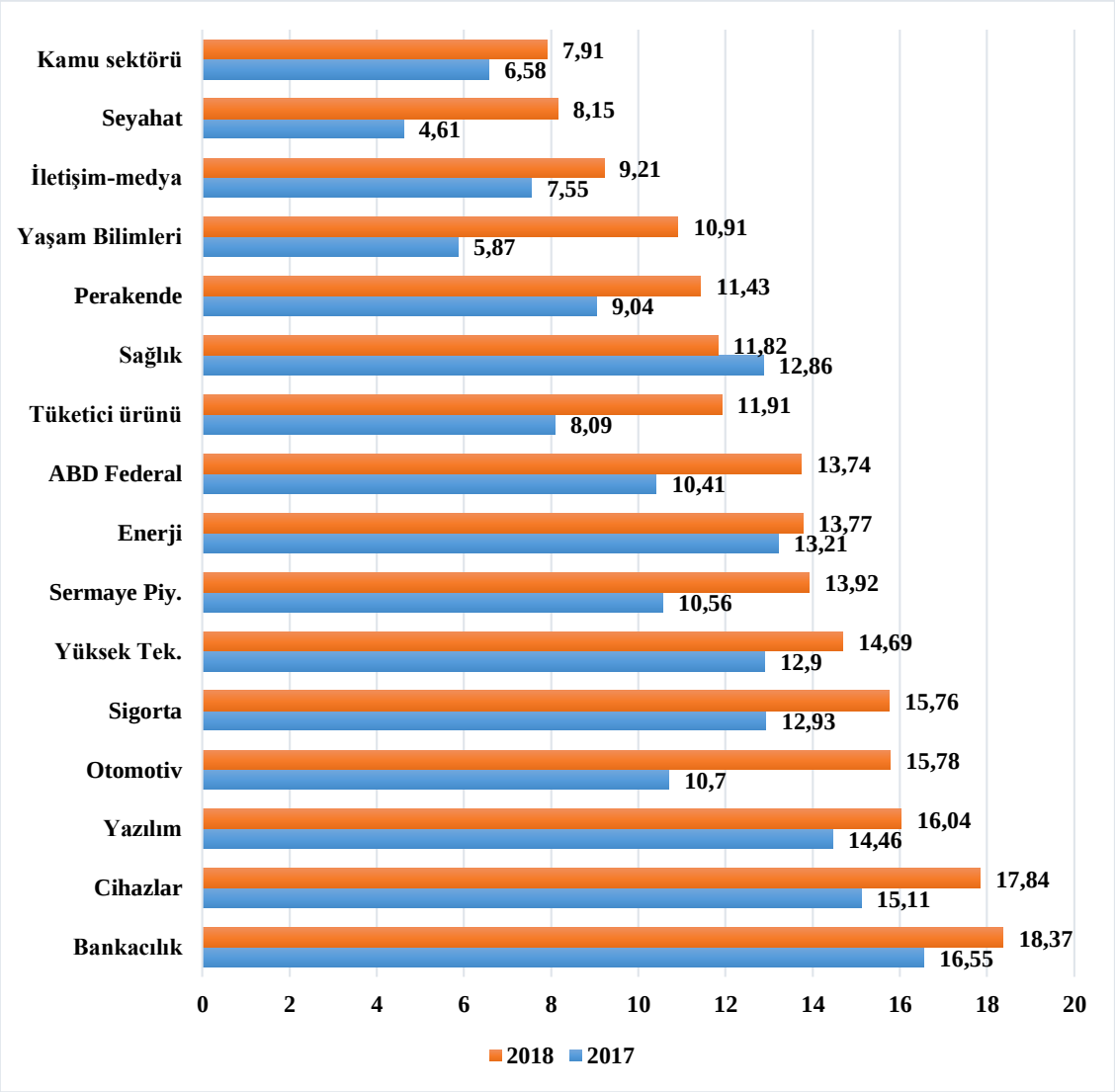
- Fidye Yazılımı (%21)
- Kötü niyetli insider (%15)
- Web Saldırıları (%13)
- Çalıntı cihazlar (%12)
- Botnetler (%12)
- Kötü Amaçlı Yazılım (%11)
- Hizmet reddi(DDOS) (%10)
- Kötü amaçlı kod (%9)
- Kimlik Avı ve sosyal mühendislik (%8)

Fidye yazılımları maliyet bakımından son sırada olmalarına rağmen artış hızı bakımından ilk sırada yer almaktadırlar. Buda gelecekte fidye yazılımlarının daha çok gündeme geleceğini göstermektedir.



Grafik 22: Siber Saldırı Türlerinin Maliyet Kategorilerine Göre Dağılımı (milyon $)
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu verileri kullanılarak tarafımızdan oluşturulmuştur.

Grafik 22'de farklı siber saldırı türlerinin maliyet kategorilerine göre dağılımı gösterilmiştir. Grafik 22'ye göre Fidye yazılımlarının, Botnetlerin, kötücül kodların, web saldırılarının, kötücül yazılımların, yemleme ve sosyal mühendislik saldırılarının en yüksek maliyetli etkisi bilgi kaybı olarak gerçekleşmektedir. Çalıntı cihazlardan ve kötücül erişimden kaynaklı en yüksek maliyet ise bilgi kaybı ve iş bozulması olarak gerçekleşmektedir.



Grafik 23: Sektöre Göre Ortalama Yıllık Siber Suç Maliyeti (milyon $)
Kaynak: Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu

Grafik 23'de siber suçların sektörlere göre yıllık ortalama maliyetleri görülmektedir. Grafik 23'de görüldüğü üzere siber saldırılardan kaynaklanan en yüksek maliyet bankacılık sektöründe gerçekleşmektedir. En az maliyetli saldırılar ise kamu sektöründe gerçekleşmektedir. 2017 yılından 2018 yılına kadar gerçekleşen siber saldırıların sağlık sektörüne olan maliyetlerinde bir azalma görülmesi de dikkat çekici bir noktadır. Sağlık sektörünün teknolojik ve bilimsel gelişmelere aciliyetle uyum sağlayan bir sektör olması sebebiyle, siber güvenlik konusunda da gerekli tedbirlerin hızla alındığı düşünülmektedir.

1.23 DEEP WEB-DARKNET-TOR İNTERNETİN KARABORSASI

Tor (onion router), ilk olarak Amerikan Donanması ile beraber, devlet içi iletişimleri korumak için geliştirilmiştir. Tor, bağlantınızın kaynağını ve istikametini gizlemek için bağlantınızı tüm dünyadan beş bini aşkın bilgisayar sunucusundan geçirir (Goodman, 2016, s:285). Ayrıca Tor browser'da bulunan bir özellik sayesinde Tor'u bilgisayarına yükleyenler de, istedikleri takdirde bilgisayarlarını Tor sunucusuna dönüştürebilmektedirler. Sivillerinde Tor sunucularını kullanmaya başlamasıyla günümüzde deep web denilen derin ağ ortaya çıkmıştır. Darknet denilen katman ise Deep web de yasadışı işler yapanların kendi aralarında daha derin ağlar kurmasıyla ortaya çıkmıştır. Darknet'e girebilmek için sadece Tor browser yeterli olmamaktadır. Farklı şifreli yönlendiriciler kullanılarak girilmektedir. Yapılan araştırmalara göre kullandığımız internet sadece buz dağının görünen yüzüdür. Tüm internet dünyasnın sadece %10'luk kısmını kullandığımız söylenmektedir geri kalan kısmı ise deep web ve darknet gibi derin ağlardan oluşmaktadır.

Tablo 6: Silk Road 2014 Ocak-Nisan

Satıcı	**Ürün**	**Toplam Ciro**
The Drug Shop	Yasadışı Ürün	6.964.776$
Heaventlos	Yasadışı Ürün	713.564
Solomio	Yasadışı Ürün	232.906
Hippie	Yasadışı Ürün	231.711
Viking King	Yasadışı Ürün	204.803
Panther Red	Yasadışı Ürün	145.450
Thebakerman	Yasadışı Ürün	140.596

Kaynak: (Bartlett, 2016, s:158)

Tablo 6'da görüldüğü üzere deep web'te bulunan yasadışı ürünler satan bir internet sitesinin birkaç aylık cirosu milyon dolarları bulmaktadır. Bunun dışında deep web'te ve darknet'te yasadışı ürünler satan yasadışı ticaret dönen yığınla internet sitesi vardır. Deyim yerindeyse darknet ve deepweb internetin karaborsasıdır.

1.24 DİJİTAL OYUN EKONOMİSİ

Küresel dijital oyun sektörü, 2011 yılsonu itibariyle 70 milyar ABD doları olarak belirlenmiştir. Bazı başyapıt niteliğindeki oyunlar, örneğin "Call of Duty: Black Ops" piyasaya sürüldükten sonraki 5 gün içerisinde 650 milyon ABD dolarına ulaşmıştır. Dijital oyunların ülkemiz içerisindeki ekonomik hacmi 150 – 200 milyon dolar olarak analiz edilmektedir(http://www.gazetebilkent.com/2015/09/22/dijital-oyun-sektorunun-gelisimi-ve-dunya-ekonomisindeki-payi/, 22.09.2018).

Ticaret Bakanı Ruhsar Pekcan, 2018 yılı oyun yazılımı ihracat rakamlarını açıkladı. Açıklamaya göre oyun yazılımı ihracatının 2018 yılında bir önceki yıla göre yüzde 50 artışla 1 milyar 50 milyon dolar olarak gerçekleşmiştir.

2018 yılında yaklaşık 138 milyar dolar seviyesinde olan küresel oyun pazarı büyüklüğünün, 2021 yılında 180 milyar dolara yaklaşacağı tahmin edilmektedir.

Bugün Türkiye'de yaklaşık 30 milyon insanın bilgisayarların, telefonların ve televizyonların başında oyun oynamaktadır.

Ülkemizdeki oyun pazarı 2017 yılında 750 milyon dolarken, 2018 yılında bu büyüklük 878 milyon dolara yükselmiştir.

Geçtiğimiz yıl dijital oyunlar pazar büyüklüğü ülkeler sıralamasında dünyada 18'inci sırada yer alan ülkemiz Orta Doğu ve Afrika bölgesinin lideri olmuştur(http://www.milliyet.com.tr/ekonomi/2018-yilinda-oyun-yazilimi-ihracati-1-milyar-50-milyon-dolar-oldu-2813693 , 18.05.2019).

Dijital oyunlar ekonomisi incelenmesi gereken ciddi bir ekonomik olguya dönüşmüştür. League Of Legends, Pubg ve CS Go gibi taraftarı bol oyunların dünya genelinde turnuvaları yapılmaktadır. Dünya genelinde meşhur olan Fortunite isimli oyun ise 2019 yılında yaptığı bir turnuvada başarılı olan oyunculara toplamda 30 milyon $ ödül dağıtmıştır. Bu para sadece oyun şirketinin turnuvada verdiği ödül miktarıdır buradan yola çıkarak oyun ekonomisinin ciddiyetini anlayabilirsiniz. Ülkemizde ve pek çok ülkede dijital oyunlar federasyonu altında Spor Bakanlığı tarafından tanınmaktadır. Bu tür oyunlarla ilgilenenlere e-sporcu sertifikaları verilerek profesyonel olarak turnuvaları gerçekleştirilmeye çalışılmaktadır. Örneğin League Of Legends isimli oyunun ülkemizde gerçekleşen turnuvaları 20.000 kişi kapasiteli Ülker Sport Arena'da yapılmıştır ve

turnuvanın izleyici biletleri kara borsaya düşmüştür. Yukarıda ticaret bakanı Sayın Ruhsar Pekcan'ın açıklamalarının yer aldığı haberde bahsedilen rakamlar oyun firmalarının elde ettiği gelirlerdir. Bunun dışında oyunların da kendi içinde ayrı bir ekonomisi bulunmaktadır. Örnek vermek gerekirse tıpkı futbol klüpleri gibi League Of Legends takımları da oyuncu transfer etmektedirler. Ve Fenerbahçe, Galatasaray, Beşiktaş gibi spor takımlarının da League Of Legends takımları bulunmaktadır. Bu büyük takımlar arasındaki transferlerde milyon dolarlık ödemeler yapılmaktadır. Bütün bunların dışında oyuncuların oyun içinde elde ettikleri, oyun araçları, geliştirdikleri oyun karakterleri gibi şeyler de ticarete söz konusu olabilmektedir. Ve bu ticaret oyun firmalarının kendi bütçelerinden çok daha büyük bir ekonomiye sahiptir. Örnek vermek gerekirse Knight Online denilen oyunda bazı oyun karakterleri veya oyun itemleri 15-20 bin lira arasında bir değere sahiptirler. Mantık olarak bu oyun içi eşyalar bitcoin gibi sanal bir değere sahiptirler, bir emeğin ürünüdürler. Son olarak bu denli ekonomik değer arz eden bir alanda elbette siber saldırılar da olmaktadır. Hacklenen oyun hesapları ciddi paralara satılmaktadır. Bu konuda da siber saldırıların ciddi ekonomik etkisi söz konusudur. Fakat siber saldırıların oyun ekonomisi üzerindeki ekonomik etkileri şöyle dursun, henüz oyun ekonomisi konusunda bile ciddi bir çalışma olmadığı için zararın boyutlarını kestirmek güçtür.

İKİNCİ BÖLÜM

SALDIRI ARAÇLARI

2.1 SIZMA TESTİ (PENETRATİON TESTİNG)

Sızma testi, belirlenen bilişim sistemlerindeki mantık hataları ve zafiyetleri tespit ederek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlemek ve sistemleri daha güvenli hale getirmek maksadıyla, "yetkili kişiler" (uluslararası akreditasyona sahip sızma testi uzmanları) tarafından ve "yasal" olarak gerçekleştirilen güvenlik testleridir. Bilgi Güvenliği ve Siber Güvenlik Danışmanlığı (Pentest hizmeti) kapsamında asıl amaç, zafiyeti tespit etmekten öte ilgili zafiyeti sisteme zarar vermeyecek şekilde istismar etmek ve yetkili erişimler elde etmektir(https://www.bgasecurity.com/danismanlik-hizmetleri/penetrasyon-testi-sizma-testi/, 5.05.2019).

2.2 SIZMA TESTİ (PENETRATİON TESTİNG) ORTAMLARI

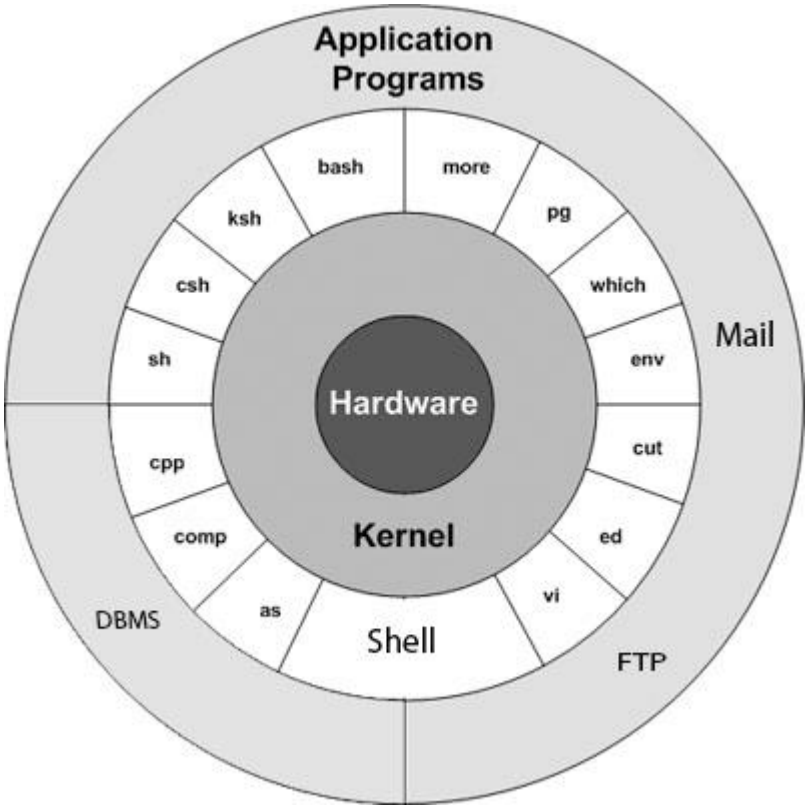
Sızma testlerinin uygulanabilmesi için içerisinde sızma testi araçlarını barındıran özel olarak bu amaca yönelik geliştirilmiş işletim sistemleridir. Bunlardan en çok kullanılanları Kali Linux, BackBox, Parrot Security OS, BlackArch, Bugtraq, Samurai Web Testing Framework, ArchStrike ve Cyborg Hawk işletim sistemleridir. Biz en çok bilineni olan Kali Linux üzerinden örneklerimizi ele alacağız.

1.8.1 Kali Linux İşletim Sistemi Sızma Testi Ortamı

Şekil 15: Kali Linux

Kaynak: Görsel Bilgisayara Kali Linux İşletim Sistemi Kurularak Alındı

Kali Linux Gnome3 ara yüzüne sahip bir işletim sistemidir. Gnome3 açık kaynak kodlu bir masaüstü ortamıdır. Linux işletim sistemi çekirdeğinin adıdır yani özel bir isimdir. Çeşitli Linux dağıtımları mevcuttur. Bunların hepsi Linux işletim sistemi çekirdeğini temel almaktadır. Ve geliştiriciler tarafından desteklenmektedir. 1991 yılında Linux ilk olarak Linus Tornvald'ın yayınladığı Linux sürümüyle başladı. Sonrasında 93 yılında şuan birçok kullanıcının kullandığı Debian yayınlandı. Akabinde Debian'ın üzerine birçok dağıtım yayınlandı. Ubuntu da bunlardan biri Linux kullanmaya başlayan birçok insan kolay kullanımından dolayı Ubuntu ile başlamıştır. Linux işletim sisteminin GNU/Linux şeklinde yazılmasının sebebi Linux'un Kamu Lisansına sahip olan bir işletim sistemi olmasından kaynaklanmaktadır. GNU'nun açılımı GNU is not Unix şeklindedir ve GNU Unix değildir anlamına gelmektedir. Linux ve Unix işletim sistemleri mimari olarak birbirlerine çok benzemektedir. Fakat bu benzerlik sadece yapısal bir benzerliktir fakat içerik olarak birbirinden farklıdırlar.



Şekil 16: Kali Linux İç Yapısı
Kaynak: https://www.micronetexperts.com/wp-content/uploads/2018/10/Capture-1.png

1.14.1.1 Linux Yapısı Ve Shell Kavramı

İçten dışa doğru Hardware> Kernel>Shell>Application Programs şeklinde bir yapıya sahiptir. Hardware(Donanım) bilgisayarımızın fiziksel kısmını yani donanımları temsil eder CPU, Bellek, hard disk gibi birimler. Bu bileşimler bilgisayarımızın fiziksel hattını oluşturur. Bu fiziksel hattın kullanıcılar tarafından kullanılabilmesi için driver gibi ara birimlere ihtiyaç vardır. Bu noktada ikinci katman olan, kernel devreye girer kernel işletim sistemimizin çekirdeğidir. İki önemli fonksiyonu vardır birisi donanım ile Application Programs(Uygulama yazılımları) arasında köprü vazifesi görmek yani bilgisayarımızın fiziksel bileşenlerinin işletim sistemine tanıtılması. Dolaylı olarak bu bileşenlerin bizler tarafından kullanılmasında rol oynar. İkinci önemli vazifesi de işletim sistemi üzerinde bellek, süreç(process(süreç) yönetimi) giriş(input) çıkış(output) gibi süreçlerin yönetilmesidir. Çeşitli dağıtımların kendilerine özgü kernelleri(çekirdekleri) vardır. Bu çekirdekler çeşitli geliştiricilerin linux çekirdeği üzerine geliştirmiş oldukları çekirdeklerdir. Kali Linux'un işletim sistemi çekirdeği de kaliye özgü bir çekirdektir ve

debian çekirdeği üzerine geliştirilmiştir. Üçüncü kısım, Shell kısmı kabuk manasına gelmektedir.

Shell(kabuk) kullanıcıların işletim sistemini kullandığı çeşitli komutlar girdiği ve bu komutların işletim sistemine iletildiği bir ara yüzdür. Bir linux işletim sistemi donanım kernel ve shell olduğu müddetçe kullanıcılar tarafından kullanılabilmektedir. Yani application programs veya diğer adı userspace kısmı olmadan da işletim sistemi kullanılabilmektedir.

Tıpkı Kernel gibi çeşitli Shell ara yüzleri bulunmaktadır. Bunlardan en çok kullanılanı bashtir. Bash ön tanımlı olarak kali linux dağıtımında gelmektedir. Shell üzerinde çalışmak için terminal denilen bir ara yüz kullanılır. Terminalde girilen komutlar shell üzerinde çalışır ve ilgili süreçlere yönlendirilir.

Açık kaynak kodlu olmasından dolayı günümüzde birçok farklı linux sürümü mevcuttur. Bu sürümler yukarıda anlattığımız üzere amaca yönelik olarak tasarlanabilmektedir. Adli bilişim amacıyla, kullanıcı odaklılık amacıyla, sızma testlerinin uygulanması amacıyla daha pek çok amaca yönelik sürümleri vardır. Ve sistem yazılımları da açık kaynak kodlu olarak gönüllü geliştiriciler tarafından geliştirilip iş yükü ve alandan tasarruf etmek amacıyla ortak linux kütüphanelerinde barındırılır. İhtiyaç halinde ihtiyaç olunan program kurulmaya hazır olarak bu kütüphanelerde bulunur. Böylece kullanılmayacak olan programlar standart olarak gelmediği için işletim sistemi az yer kaplar.

2.3 HACKİNG METODOLOJİSİ

Hacking metodolojisi beş aşamadan oluşmaktadır.

1- Keşif Aşaması

Keşif aşamasında hacklenilecek hedef hakkında her yoldan bilgi toplanılmaktadır. Bu aşamada, hedef alınan sistemin adı(domain name), işletim sistemi bilgileri, erişim sağlanacak olan ana bilgisayarların(hostlar) ve router'ların konumları, açık portlar, işletim sistemi ve sistemde çalışan diğer servisler hakkında ayrıntılı bilgiler elde edilmeye çalışılır (Henkoğlu, 2014, s:169)

Keşif kendi arasında aktif keşif ve pasif keşif olmak üzere ikiye ayrılır.

Aktif keşif: Bilgi toplarken hedef web sunucusu üzerinde iz bırakarak, hedef web sunucusu ile doğrudan temasta bulunularak bilgi elde etme aşamasına aktif bilgi toplama denir (Çıtak, 2018, s:20). Aktif keşfi hedefle her türlü teması kapsar yerine göre hacklenen hedefle fiziksel temas gerektiği durumlarda aktif keşiftir.

Pasif Keşif: Hedefle herhangi bir doğrudan temas kurmadan iz bırakmadan Whois, Lookup gibi domain veri tabanları üzerinden bilgi toplama yöntemine pasif keşif denilmektedir(Çıtak, 2018, s:20).

2-Tarama Aşaması

Keşif aşamasında edinilen bilgiler kullanılarak sızma testi araçları veya hacking araçları ile sistemde çeşitli zafiyet taramaları yapılır ve sistemde bir açık bulmaya çalışılır.

3-Erişim Kazanma

Tarama aşamasında tespit edilen açıklar kullanılarak hedef sisteme erişim sağlanmaya çalışılır. Yüksek risk seviyesinde görülen bu aşamada, hedef alınan sistemde meydana gelebilecek zararın boyutu, hedef sistemin yapısı ve konfigürasyonuna, sistem üzerinde kazanılan erişim düzeyine ve saldırıyı yapan kişinin becerisine göre değişebilmektedir (Henkoğlu, 2014, s:170).

4-Erişimi Sürdürme Aşaması

Hedef sisteme erişim sağlandıktan sonra, sağlanan erişimin sürdürülebilmesi için yetki arttırımı ve açıkları kapatmak gibi önlemler almaya erişimi koruma aşaması denilmektedir. Yetki arttırımı sistemde yönetici olmaya çalışmaktır. Açıkların kapatılmasının amacı da başka hackerlar veya sızdığımız sistemin kendi güvenlik sistemleri tarafından açıkların tespit edilerek sistemdeki varlığımızın anlaşılmasını engellemektir. Sistem sahipleri bir açık tespit etmeleri durumunda yetkisiz erişim taraması yapacaklardır ve bizim varlığımızdan haberdar olacaklardır açıkları kapatmak bu yüzden önemlidir.

5-Delilleri Silme

Delilleri silme aşaması, hackerların hedef aldıkları sistemi kendi amaçları doğrultusunda kullandıktan sonra sistem üzerinde yaptıkları değişikliklerin ve etkinliklerin tespit edilmesini önlemek amacıyla yaptıkları çalışmaları içerir. Bu aşamada

yapılan çalışmaların amacı, yapılan dair delilleri yok ederek yasal sorumluluktan kaçınmaktır(Henkoğlu, 2014, s:170).

2.1.1 Gelişmiş Israrcı Tehdit-Advanced Persistent Threat (APT)

Gelişmiş ısrarcı tehditler bir tür hacking yöntemini ifade eder. Bir sisteme izinsiz erişim sağlayan grup ya da kişi uzun süre izini belli etmeden sistemde kalır ve bilgi toplar. Sonrasında en uygun zamanı kollayarak vurucu saldırısını gerçekleştirir. En büyük ekonomik sonuçlar doğuran saldırılar arasındadır. Fakat anlatıldığı üzere teknikten dolayı fark edilmeleri çok güçtür.

2.4 ÇÖPE DALMAK

Çöpleri karıştırarak çöpe atılmış olan şirket telefon rehberi, kısa notlar, şirketin idari politika bilgileri, olaylar ve tatil izinleri, sistem işleyiş şekilleri, hassas veriler ya da giriş isim ve şifreleri çıktıları, kaynak kod çıktıları, diskler ve bantlar, şirket mektupları ve kısa formlar ve eskimiş donanımlar gibi çöplerden hedef hakkında bilgi elde etmektir.

Bu kaynaklar hackerlar için zengin bilgi damarlarıdır. Telefon rehberleri hackerlara hedefteki insanların telefon numaralarını ve isimlerini verir. Organizasyon grafikleri organizasyondaki yetkili pozisyondaki kişiler hakkında bilgiler içerir. Küçük notlar giriş oluşturmak için cazip ve ilginç ufak bilgiler içerir. Takvimler çok önemlidir, hangi işçinin ne zaman işyeri dışında olacağını belirtir. Sistem el kitapları, hassas bilgiler ve diğer teknik bilgi kaynakları hackerlara ağa izinsiz girebilmek için gerekli bilgileri verebilir. Son olarak, eski donanımlar özellikle hard diskler yeniden onarılıp tüm kullanışlı bilgiler elde edilebilir (https://www.cyber-warrior.org/dokuman/Default.Asp?Data_id=4442, 10.6.2019).

2.5 SOSYAL MÜHENDİSLİK

Sosyal mühendislik saldırılarında şüphesiz en meşhur kişi, Pentagon, Sun Microsystems, Motorola gibi pek çok kuruluşa saldırarak FBI'ın en çok arananlar

listesine giren ilk siber korsan Kevin Mitnick'tir. Şu anda "güvenlik uzmanı" olarak çalışmaktadır (Çifci, 2017, s:166)

Sosyal Mühendislik Döngüsü

Araştırma: *Güvenlik delme testi kayıtları, yıllık raporlar, pazarlama broşürleri, patent uygulamaları, basın kupürleri, sektör dergileri, internet sayfası içeriği ve çöpe dalınarak elde edilen bilgiler gibi şeyleri araştırmaktır.*

Dostluk ve güven uyandırma: *içeriden gelen bilgilerin kullanılması başkasının kimliğine bürünme, kurbanın tanıdığı kişilerin adlarının sıralanması, yardım isteği ya da otoriteye sahip olma.*

Güveni kötüye kullanma: *Kurbandan, bir bilgi vermesinin ya da bir işlem yapmasının istenmesi.*

Bilgi kullanma: *Eğer edinilen bilgi asıl amaçtan bir adım uzaktaysa, saldırgan, amacına ulaşana kadar önceki adımlara geri döner* (Mitnick & Simon, 2017, s:303).

Sosyal mühendislik hedef hakkında çeşitli yöntemlerle elde ettiğimiz verileri kullanarak, yetkili biri, bir iş arkadaşı veya arkadaşının arkadaşı gibi bir izlenim bırakıp hedef kişiden normalde vermemesi gereken bir bilgi almak veya normalde yapmaması gereken bir şey yapmasını sağlamaktır.

2.6 OLTALAMA-YEMLEME (PHİSHİNG)

Kişiye özel bilgileri ve şifreleri ele geçirme amacıyla hazırlanan zararlı yazılımlardır. Genellikle e-posta yoluyla hedefteki kişiye ulaşılır ve gelen e-posta orijinal kaynağının ayırt edilmesi çok güç olacak kadar benzeridir. Banka bilgilerine ulaşmak amacıyla yaygın olarak kullanılan phishing e-postaları, kullanıcıların girdiği bilgileri sahte adrese taşır (Henkoğlu, 2014, s:190).

2.7 KLAVYE KAYDEDİCİLER (KEYLOGGERLAR)

Keyloggerlar bulaştıkları sistemde verileri kaydedip raporlayıp belirlenen bir adrese gönderen veya sonra alınması üzere kaydeden yazılımlardır. Donanım olarak çalışan keyloggerlar da vardır, donanımsal keyloggerların sisteme fiziksel olarak entegre edilmesi gerekmektedir. Aslında bu yazılımlar kötü amaçlara alet olsunlar diye yazılmamışlardır. Bir şirket yöneticisi çalışanlarının kendi işinden başka işlerle ilgilenmesini engellemek, bir ebeveynin çocuğunun zararlı sitelere girmesini engellemek ve girdiği yerleri görmek için keylogger yazılımlarından istifade ederler (Elbahadır, 2017, s:109). Günümüzde hackerlar tarafından sıkça kullanılan keyloggerlar oldukça gelişmiş vaziyettedirler.

Kuruldukları sistemin klavye girdilerini, anlık ekran görüntülerini, sistem kayıtlarını, program açılış ve kapanış saatlerini, çalınan müziklerin isimlerini, sosyal medyada sohbet edilen kişilerin isimlerini bile raporlamaktadırlar (Çıtak, 2018, s:124).

2.8 TRUVA ATLARI & RAT'LAR

Truva savaşında düşmanların tahta at heykelinin içine girerek şehri ele geçirmelerinden esinlenerek bu ismi almıştır. Trojenler başka yazılımların içine saklanan bir çeşit zararlı yazılımdır. Örneğin ücretli bir yazılımın, kırılmış ücretsiz hale getirilmiş ve internete yüklenmiş versiyonlarının içine sıkça trojen yerleştirilmektedir. Bu yazılımı ücretsiz olarak indiren kişilerin bilgisayarına bulaşan trojen arka planda çalışarak saldırgana bir erişim yolu açar ve bu erişim sayesinde bilgisayarlar zombi bilgisayar dediğimiz ele geçirilmiş bilgisayarlara dönüşür. Sonrasında saldırganlar bu tür ele geçirdikleri bilgisayarları kullanarak DDOS saldırıları yapmak gibi çeşitli hacking faaliyetleri yürütürler. Trojenlerin uzaktan yazılım yüklemeye izin veren gelişmiş versiyonlarına ise Remote Access Trojan (RAT) denilmektedir. RAT'lar bulaştıkları sistemde merkezle uzaktan erişim sağlayarak başka zararlı yazılımların yüklenmesine de aracılık edebilecek kabiliyete sahiptirler. Trojanlar ise bulaştıkları sistemlerde sadece merkezden gelen komutları işletebilecek kabiliyettelerdir.

2.9 DDOS (DAĞITIK HİZMET DIŞI BIRAKMA SALDIRISI-DİSTRİBUTED DENİAL OF SERVİCE)

DDOS saldırıları bir çeşit hizmet dışı bırakma saldırısıdır. İnternet siteleri sunucu dediğimiz özel bilgisayar sistemlerinde barındırılır. Biz bir internet sitesini ziyaret ettiğimiz zaman, bizim bilgisayarımızdan internet üzerinden ziyaret ettiğimiz internet sitesinin barındırıldığı sunucu bilgisayara, bir istemci paketi gönderilir. Sunucu bilgisayar da karşılık olarak bir onay paketi gönderir. Sonrasında bağlantı kurulur ve veriler internet protokolü üzerinden (Hyper Text Transfer Protocol) http kısaltması olan bir protokol üzerinden HTML (Hyper Text Markup Language) denilen bir dil temelinde iletilir. DDOS saldırılanda ise sunuculara görüntüleme isteği gönderen fonksiyonlar saniyede binlerce kez olabilecek şekilde zombi bilgisayar denilen ele geçirilmiş bilgisayarlar üzerinden aynı anda defalarca gönderilir. Bunun sonucunda örneğin saniyede 10.000 görüntüleme isteğine yanıt verebilecek bir sunucu görüntüleme isteklerine yanıt veremez hale gelir. Ve saldırı yapılan sitenin gerçek ziyaretçileri siteyi ziyaret etmek istediklerinde ulaşamazlar. Site hizmet veremez hale gelir. Bu tür saldırılara dağıtık hizmet dışı bırakma saldırısı denilmektedir.

2.10 SIFIRINCI GÜN SALDIRILILARI (0-DAY)

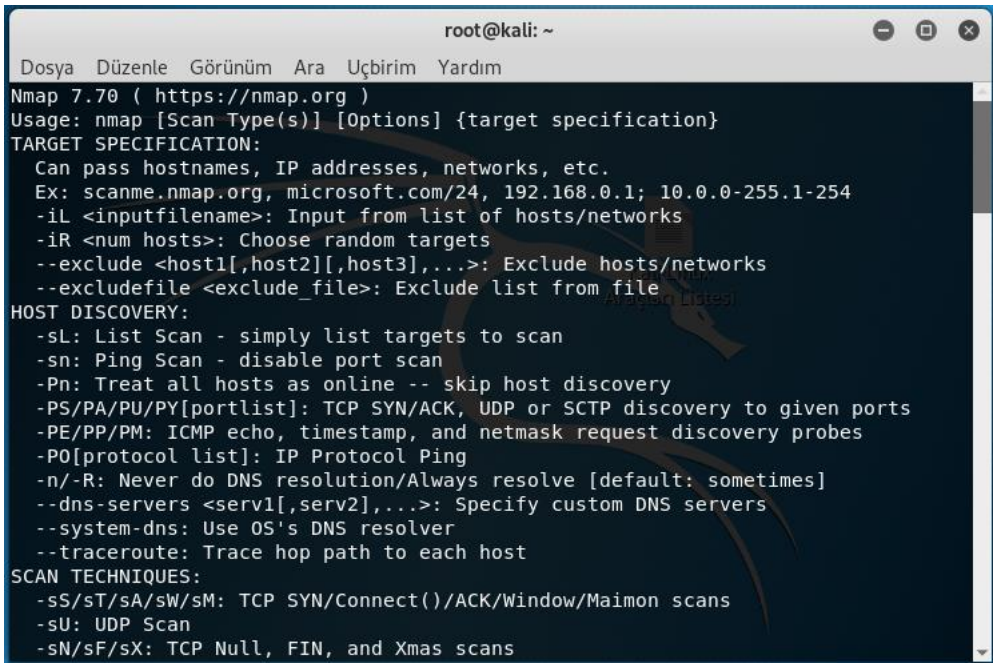
Sıfırıncı gün açığı bir sistemde bulunan bir açığı başkaları keşfetmeden keşfedip kullanmak veya herkesten önce tespit etmek anlamında kullanılan bir terimdir. Hackerlar en tehlikeli saldırıları bu tür açıklardan faydalanılarak yapmaktadırlar. Önceleri bu tür açıkları Microsoft gibi ilgili firmalara bildirerek açıkların kapanmasını sağlayan hackerlar bildirimleri karşılığında gözle görülür bir ödül alamadıkları için sonrasında bu tür açıkları kullanarak çıkar elde etmeye ve hatta bu tür açıkları Darknet'te bulunan 0-day karaborsalarında satmaya başlamışlardır. Bu tür henüz kimse tarafından tespit edilmemiş açıkların maddi değeri oldukça fazladır. Stuxnet örneğinde de saldırganlar 4 adet daha önce görülmemiş 0-day açığını tek seferde kullanmışlardır.

2.11 SALDIRI ARAÇLARI LİSTESİ

Kali Linux kütüphanesinde yüzlerce sızma testi aracını ve adli bilişim aracını barındırmakla beraber bu araçlar çeşitli kategorilere ayrılmıştır menüler altında verilmiştir. Aşağıda Kali Linux Sızma Testi ortamının menüleri verilmiştir. Örnek olması açısından bu menüler altında bulunan sızma testi araçlarının hacking metodu olarak veya sızma testi amacıyla nasıl kullanıldığına dair genel bilgiler verilecektir. Yer kaplamaması bakımından programların görselleri verilmemiştir. Sadece örnek teşkil etmesi için Nmap aracının görseli verilmiştir. Diğer programlarında birçoğu aynı şekilde terminal ara yüzünde çalışmaktadır.

1- İnformation Gathering (Bilgi Toplama)
2- Vulnerability Analysis (Güvenlik Açığı Analiz Araçları)
3- Wireless Attacks (Kablosuz Ağ Saldırısı)
4- Web Applications (Web Uygulama Araçları)
5- Exploitation Tools (Zafiyet Sömürme Araçları)
6- Stress Testing (Stres Testi Araçları)
7- Sniffing & Spoofing (Ağ Dinleme Ve Sızma Araçları)
8- Password Attacks (Parola Saldırı Araçları)
9- Maintaining Access (Erişimi Koruma Araçları)
10- Reverse Engineering (Tersine Mühendislik Araçları)
11- Hardware Hacking (Donanım Hackleme Araçları)
12- Forensics Tools (Adli Bilişim Araçları)
13- Reporting Tools (Raporlama Araçları)

2.12 NMAP AĞ KEŞFİ ARACI



Şekil 17: Nmap aracından bir görüntü
Kaynak: Kali Linux'tan alınmıştır

Ağ haritalama aracıdır sistem yöneticileri tarafından ağları keşfetmek ve güvenliklerini denetlemek için kullanılan ücretsiz ve açık kaynaklı bir yardımcı araçtır. *[nmap --script vuln site veya ıp adresi]* komutu ile çalıştırılır. Scriptleri görmek için farklı bir komut satırı penceresinde *[locate *.nse]* komutu ile nmap'ın içerisindeki scriptleri görebiliriz. Bu scriptelerin arasından vuln (Vulnerability) zafiyet taraması için kullanılandır. Zafiyetleri taradıktan sonra zafiyetlerle ilgili detaylı bilgi bulunabilecek siteleri de paylaşıyor.

2.13 GOLİSMERO ARACI

Uygulamalar/Zafiyet Analizi Araçları/golismero menüsü altında bulunmaktadır. *[golismero.py scan hedef url adresi]* komutu ile terminalden çalıştırılmaktadır. Birçok aracı içinde barındıran bir programdır içinde bulundurduğu araçlarla sırasıyla zafiyet taramaları yapmaktadır. Kullandığı araçları liste halinde kullanırken göstermektedir. Komut çalıştırıldığında en son hangi araçla ne tür bir açık bulduğunu düzenli bir liste şeklinde sunmaktadır.

2.14 LYNİS ARACI

Uygulamalar/Zafiyet Analizi Araçları/Lynis menüsü altında bulunmaktadır. Lynis linux ve unix tabanlı sistemleri denetlemek için hazırlanmış bir programdır. Bu sistemlerdeki yüklü programları tarayıp olası yapılandırma sorunlarını bulmak için yapılandırılmıştır.

[Lynis audit System] komutu kendi yerel ağımızda tarama yapmaktadır.

[Lynis audit System remote] komutu da hedef ağda tarama yapmaktadır.

2.15 NİKTO ARACI

Uygulamalar/Zafiyet Analizi Araçları/Nikto menüsü altında bulunmaktadır.

[nikto -h hedef site veya ıp] komutu ile çalıştırılır. Zafiyet açığı tespit ettiği takdirde sonuçları kodlarla sıralamaktadır. Sıralanan kodları internette arama motorlarında arattığımızda açıklarla ilgili detaylı bilgilere ulaşılarak tespit edilen açıklar kullanılmaktadır. Bu uygulama pentest ortamı kurulduğu zaman genelde test amaçlı zafiyet barındıran sanal bir sunucu üzerinde denenmektedir.

2.16 NİX-PRİVESC-CHECK ARACI

Uygulamalar/Web Uygulama Analizi Araçları /Unix-Privesc-Check menüsü altında bulunmaktadır.

[unix-privesc-check standart] standart tarama komutu

[unix-privesc-check detailed] detaylı tarama komutu

Olmak üzere iki farklı tarama modu mevcuttur. En iyi tarama sonucu için root(yönetici) yetkisinde çalıştırılmalıdır. Daha çok sunucularda kullanılan bir araçtır. Bu programın amacı bir sistemde root yetkisine sahip olmaması gereken farklı kullanıcılar olup olmadığını tespit etmektir. Tarama sonuncunda warning(tehlike) uyarısı verdiği takdirde uyarı kodunu verdiği dosya ile ilgili bir yetkilendirme sorunu olduğu anlamına gelmektedir. Bu tür dosyalarla ilgili yetki düzenlemesi yapılması gerekmektedir.

2.17 BURP SUİTE ARACI

Uygulamalar/Web Uygulama Analizi Araçları/Burp Suite menüsü altında bulunmaktadır.

Hem demo hem de ücretli bölümü bulunmaktadır. Next>start>burp adımlarını izleyerek programı çalıştırıyoruz. Proxy bölümü kullanılarak araya girme saldırıları Man İn The Middle (MITM) saldırıları ve içinde barındırdığı menülerle pek çok saldırı yapılabilmektedir. Bu yüzden yasal sorumluluktan dolayı detaylı olarak anlatılmayıp sadece nasıl çalıştığına yönelik genel bilgiler verilecektir.

Bir web sitesini açtığımız zaman giden gelen verilere gidiş dönüş şekillerine göre işlemler gerçekleştirilir. Pentest işlemlerin sağlıklı işlemesi için istemci ile sunucu arasında yapılan her işlemin gerek istemciden çıkıp sunucuya varmadan kontrolü gerekse de sunucudan istemciye dönen cevap istemciye varmadan araya girerek bakılması çok önemlidir. Burp Suite işte burada devreye girer çalışma mantığı web sitesi ile sunucu arasına girip verileri tekrar kendi üzerinden sunucuya göndermek şeklindedir.

2.18 COMMİX ARACI

Uygulamalar/Web Uygulama Analizi Araçları/Commix menüsü altında bulunmaktadır. Bu araçta sızma testi alıştırmalarında bünyesinde açık barındıran bir sunucu sanal makineye kurularak denenmektedir. Açıklı sunucunun komut satırında ifconfig komutu ile sunucunun ıp adresini öğreniyoruz. Daha sonra commix aracı ile komut enjeksiyon zafiyeti tespit ettiğimiz dosyanın url sine *[commix --url=açık bulunan dosyanın url adresi INJECT_HERE]* komutlarını kullanarak komut satırı zafiyeti enjekte ediyoruz.

Yukardaki komut kullanıldıktan sonra commix kontrol edip terminaline ulaşılsın mı diye soruyor y(evet) diyoruz. Bu araç kullanılarak sitenin komut satırı ekranına ulaşabiliyoruz. Daha sonra ls komutu ile bulunduğumuz yerdeki dosyaları listeleyebiliriz cat komutu ile dosyaları okuyabiliriz veya yetkimize göre komut satırı kodları ile işlemler yapabiliriz.

2.19 HTTRACK

Uygulamalar/Web Uygulama Analizi Araçları/Httrack menüsü altında bulunmaktadır.

Bu uygulama bir internet sitesinin olduğu gibi kopyasını alan bir programdır. Çalıştırıldığında yardım menüsü ile birlikte çalışmaya başlamaktadır, *[httrack]* komutu ile çalıştırılmaktadır. Çalıştırıldığında bize bir proje adı soruyor üzerinde çalışacağımız projenin ismini giriyoruz. Sonra kaydedileceği yolu soruyor ve kaydedileceği yeri de gösterip onaylıyoruz(enter tuşuna basıyoruz). Daha sonra hangi sitenin tamamı alınacağını soruyor bu bir ıp adresi de olabilir bir internet sitesi de //http:192.176.100 vs gibi.

Hedefi belirttikten sonra bize bazı seçenekler sunuyor

1. Olduğu gibi alıyor mirror web
2. Bir sihirbaz yardımıyla hepsini alıyor
3. Belirlenen dosyaları just get files
4. Bütün linklerle birlikte miror all links
5. Test edilmiş linkleri alıyor

Birini seçip onayladıktan sonra bir proxy kullanılıp kullanılmayacağını soruyor kullanacaksak giriyoruz kullanmayacaksak onaylayıp geçiyoruz. Sonra belli dosya formatları soruyor seçim yapacaksak giriyoruz gif,jpeg vs. yapmayacaksak onaylayıp geçiyoruz. En son işlemi başlatmak için y/n soruyor y ye basıp onaylıyoruz.

2.20 OWASP ZAP ARACI

Uygulamalar/Web Uygulama Analizi Araçları/Owasp zap menüsü altında bulunmaktadır.

Web sitelerindeki güvenlik zafiyetlerini tespit eden bir araçtır. Araç bir kullanıcı ara yüzü ile geliyor. Arayüzde saldırı url bölümüne direkt hedef adres girilip saldırı başlatılmaktadır.

- Sites bölümünde sitenin sayfaları tespit edilmektedir.
- Uyarılar bölümünde de sayfalardaki açıklar tespit edilip listelenmektedir.

- Active scan bölümünden taramanın durumu kontrol edilebilmektedir.

Commix te kullanılan uzaktan komut enjeksiyonu açığının adresi bu tür programlar sayesinde tespit edilmektedir. Tespit edilen zafiyetlerin detaylarına baktığımızda sağda url yazan yerde zafiyetin kullanılmış halini de vermektedir.

2.21 PAROS ARACI

Uygulamalar/Web Uygulama Analizi Araçları/ Paros menüsü altında bulunmaktadır.

Yaklaşık 10-12 yıldır geliştirme yapılmamış bir programdır. Program işlevini düzgün bir şekilde yerine getirememektedir. Tarayıcı üzerinden proxy ayarı gerçekleştirilerek çalıştırılmaktadır. Program proxy üzerinden tarayıcı ile eş zamanlı olarak çalıştırılmalıdır. Proxy ayarlarını yaptıktan sonra tarayıcıdan sayfayı yeniliyoruz ve program çalışmaya başlıyor. Daha sonra programdan analiz ve scane seçeneklerinden taramayı başlatılır ve ziyaret edilen internet sitelerinde bulabildiği açıkları listelemektedir.

2.22 SKİPFİSH ARACI

Uygulamalar/Web Uygulama Analizi Araçları/skipfish menüsü altında bulunmaktadır. Web uygulamalarındaki zafiyetleri tespit eden bir araçtır bunun yanında resim dosyalarını da tespit edebilmektedir. Tarama işlemini komut satırı üzerinden yapılmaktadır fakat sonuçları bize görsel olarak göstermektedir. Elde edilecek sonuçların kaydedileceği dosyanın yolu [skipfish –o] komutu ile kaydedilmektedir.

Kullanımı [skipfish -o root/Desktop/sitetarama http://192.168.1.105(hedef adresi)] komutu girilip onaylandıktan sonra 60 saniye içinde tekrar onay istemektedir. Tekrar onaylayıp devam ediyoruz. Tarama tamamlandıktan sonra tarma sonuçları dosyamıza gidiyoruz “index.html” dosyasını açtığımızda sonuçları bize bir internet sayfası görünümünde bize göstermektedir.

2.23 SQLMAP ARACI

Uygulamalar/Web Uygulama Analizi Araçları/sqlmap menüsü altında bulunmaktadır.

SQL açığı bulunan sitelerde veri tabanına ulaşmamızı sağlayan bir araçtır. Çalışır çalışmaz komut yardım ekranı karşımıza gelmektedir. *sqlmap -u http://hedefadresi --dbs*

--dbs parametresi sitenin veri tabanı ismini öğrenme amacı ile eklenen bir parametredir.

Eğer hata verirse örneğin: [*switch '--random agent'*](random agent parametresini ekleyin) gibi bir hata verirse eklenmesi istenen parametre komuta eklenilip tekrar çalıştırılır.

sqlmap -u http://hedefadresi --dbs --random agent

Listelenen veri tabanı sonuçlarından "information schema" ismi varsayılan olarak her veri tabanına verilen isimdir.

sqlmap -u http://hedefadresi -D –veri tabanı ismi --tables --random agent (falanca isimli veri tabanı içindeki tabloları listele)

Tablolar listelendikten sonra: *[sqlmap -u http://hedefadresi -D –veri tabanı ismi -T istenilen tablo --columns --random agent]* (falanca isimli veri tabanındaki falanca toblodaki kolonları göster).

Kolonlar listelendikten sonra: *[sqlmap -u http://hedef adresi -D –veri tabanı ismi –T] istenilen tablo -C yazdırılacak kolon --dump --random agent* (falanca isimli veri tabanındaki falanca tablodaki falanca kolonu yazdır).

Bu şekilde user ve password vs. gibi tablolar varsa veya işimize yarayacak bilgileri içeren tablolar bu şekilde yazdırabilmektedir.

2.24 WEBSCARAB ARACI

Uygulamalar/Web Uygulama Analizi Araçları/webscarab menüsü altında bulunmaktadır.

Görsel ara yüzlü bir programdır birkaç özelliği bulunmaktadır. Bunlardan bir tanesi proxy özelliği proxy özelliği sayesinde burbsuite de gerçekleştirdiğimiz araya

girme işlemleri gibi işlemler gerçekleştirilmektedir. Fakat programın en verimli özelliği spider özelliği ile link yakalamadır. Tarayıcıdan öncelikle proxy ayarlarını gerçekleştiriyoruz.

Proxy ayarlarını yapmak için programdan proxy/listeners menüsüne bakılıp programın kullandığı proxy ve porta bakılır ve aşağıdaki örnekteki gibi tarayıcı ayarları yapılır.

Pereferences/Advenced/network/settings/manuel proxy:127.0.0.1 port:8008

Bu işlem sayesinde yaptığımız her işlem önce programa gidecek daha sonra programdan sunucuya yollanacaktır. Bu işlemler yapıldıktan sonra tarayıcıdan hedef siteye girilir.

Siteye girildikten sonra program link yakalama işlemine başlamaktadır.

2.25 WPSCAN ARACI

Uygulamalar/Web Uygulama Analizi Araçları/Wpscan menüsü altında bulunmaktadır.

Bu araç çalıştırıldıktan sonra güncelleme yapılsın mı diye sorar y ye basıp enter a basıp onaylamalıyız yoksa hata alabiliriz. Wordpress sitelerde bilgi toplama ve kaba kuvvet saldırıları için kullanılan bir araçtır.

wpscan --url hedefwpsitesi --enumarate u (yöneticinin kullanıcı adını tespit ediyor)

wpscan --url hedefwpsitesi --enumarate t (sitede kullanılan temayı tespit ediyor)

wpscan --url hedefwpsitesi --enumarate p (sitede kullanılan eklentileri tespit ediyor)

Örneğin yönetici kullanıcı adını tespit edip o kullanıcı adına kaba kuvvet saldırısı yapmak için:

Yönetici kullanıcı adı tespit edildikten sonra *[wpscan --url hedefwpsitesi --username logintablosundayazankullanıcıadı --wordlist /oluşturduğumuz/wordlistin/yolu]*

Yukarıdaki komutu verdikten bir süre sonra "Do you want to start the brute force anyway?" diye sorduğunda “y” deyip onaylayınca kaba kuvvet saldırısı başlayacaktır.

2.26 JSQL İNJECTİON:

Uygulamalar/Database Assessment/JSql İnjection menüsü altında bulunmaktadır.

Görsel ara yüzlü bir programdır ve sql zafiyeti bulunan veri tabanlarını ele geçirmek için kullanılan bir programdır. Açıklı sitenin linkini kopyalayıp programa yapıştırıp giriş tuşuna basıyoruz. Program ilk hamle olarak açıklı sayfayı kullanarak veri tabanı isimlerini tablolarını kolonlarını ve veri tabanı bilgilerini listeleyecek. Aşağıdan ağ bölümünden yapılan işlemleri görebiliriz program açıklı sayfa üzerinden komutları çalıştırarak sonuçları listeliyor.

Kolsol bölümünden done ibaresini görene kadar bekliyoruz done ibaresi işlemini tamamladığını belirtir. Tarama işlemi bittikten sonra veri tabanı ismine tıklıyoruz burada bize veri tabanının bütün tablolarını listeliyor. Daha sonra inceleyeceğimiz tablo ve kolonu tıklayarak ilerliyoruz. Örneğin Users tablosu altında pssword usurname users ıd vs gibi kolonları seçiyoruz. Daha sonra bu kolonların bağlı olduğu users tablosuna sağ tık yapıp threat yükü seçeneği ile bilgileri görüntülüyoruz.

2.27 SİDGUESSER ARACI

Uygulamalar/Database Assessment/SidGuesser menüsü altında bulunmaktadır.

Kaba kuvvet saldırısıyla oracle veri tabanlarındaki kullanıcı adlarını tespit etmeye çalışan bir program bunun için bir Word liste(deneme listesi) ihtiyaç duymaktadır. Terminalde çalışan bir program hedef veri tabanı ıpsi ve wordlist yolu belirtilerek kullanılmaktadır.

2.28 SQLDİCT

Uygulamalar/Database Assessment/SQLDict menüsü altında bulunmaktadır.

Görsel ara yüzlü bir programdır. Sql sunuculara kaba kuvvet saldırısı gerçekleştiren bir program bunun için bir Word liste ihtiyaç duymaktadır. Oldukça eski bir uygulamadır 2000 yılında yapılmış bir uygulama olmasına rağmen hâlâ işlevini sürdürmektedir. Sunucu bulmak için www.shodan.io sitesinden “sql server” diye arama

yaparak bir sql sunucu bulunur. Oradan bir sql server bulup ıp adresini programa yapıştırıyoruz target account kısmına “administrator” yazıyoruz. Load Password File kısmından da hazırladığımız wordlisti gösterip programı çalıştırılır.

2.29 SQLİTE DB BROWSER

Uygulamalar/Database Assessment/SQLite DB Browser menüsü altında bulunmaktadır.

Bu program veri tabanı oluşturmaya ve var olan veri tabanlarını açmaya yarayan bir programdır. Önce bir veri tabanı açıp bir takım değerler girip inceleyelim.

Yeni veri tabanı diyoruz nerede oluşturulacağını seçiyoruz ve ismini veriyoruz ve uzantısını db yapıp save deyip kaydediyoruz. Kaydettikten sonra bize tablo adı vermemiz için bir ekran açıyoruz buraya bir tablo adı vererek bir tablo oluşturuyoruz. Alan ekle kısmından da kolonları ve verilerin tutulacağı yerleri belirtiyoruz. Gerekli alanları oluşturup tamam dedikten sonra programın ana ekranında üst menüde write changes seçeneğinden değişiklikleri kaydetmesini sağlıyoruz. Daha sonra browser data sekmesinden yeni kayıt diyerek seçili alanlara gerekli bilgileri girebiliyoruz. Bu program ile bu şekilde bir veritabanı oluşturabiliyoruz. Elimizde hazırda bulunan veri tabanlarını açmak içinse programın ana ekranında bulunan veri tabanı aç seçeneğini kullanarak açabiliyoruz.

2.30 THE MOLE

Bu programı kurmak için öncelikle *[apt -get install themole]* komutunu girerek linux deposundan indirmek gerekmektedir. Themole programı kurulduktan sonra komut satırından themole diyerek programı çalıştırıyoruz. Program çalıştıktan sonra açıklı site linkini kopyalayıp *[url açıklı site linki]* şeklinde programa giriyoruz. Daha sonra program bizden hedef adresten bir kelime istiyor. Hedef sitedeki başlıklardan herhangi birini kopyalayıp *[neddle kopyalanan kelime]* komutunu giriyoruz.

Ardından da schemas komutunu girerek bu zafiyeti kullanarak veri tabanı isimlerini elde etmesini bekliyoruz. Program bize veri tabanı isimlerini tespit ettikten

sonra. Veri tabanının tablolarını görüntülemek için *[Tables veri tabanı ismi]* komutunu giriyoruz. *columns veri tabanı ismi tablo ismi* komutunu girerek kolonları görüntülüyoruz. *query veri tabanı ismi tablo ismi kolon ismi, kolon ismi2,* şeklinde görüntülemek istediğimiz kolonların isimlerini aralarına virgül koyarak sıralıyoruz.

2.31 TNSCMD10G

Uygulamalar/Database Assessment/TnsCmd10g menüsü altında bulunmaktadır.

Bu araç Oracle veri tabanlarında bilgi toplamaya yarayan bir araçtır.

www.shodan.io sitesinden oracle yazarak bir oracle veri tabanı aratıyoruz çıkan oracle veri tabanlarından details kısmına tıklayarak 1521 portunun açık olup olmadığına bakıyoruz. Çünkü oracle varsayılan olarak 1521 portunu kullanıyor.

Siteler arasından tek tek 1521 port açık site aramak zor olacaksa gene shodan.io üzerinden port 1521 diye aratabiliriz. Daha sonra shodan.io nun 1521 portu açık olarak bize listelediği sitede oracle kurulu olduğundan emin olmak için Kali Linux terminalinde.

nmap -sS -sV hedefıp komutu ile portları ve servisleri kontrol edebiliriz.

Veya hedef sitede çok fazla açık port varsa ve tarama uzun *sürecekse [nmap -sS -sV -p 1521 hedef ıp adresi]* komutu ile sadece 1521 komutunu kontrol edebiliriz.

Bu kontrolleri yaptıktan sonra TnsCmd10g programını açıyoruz.

tnscmd10g version -h hedef ıp komutu ile sürüm bilgisini

tnscmd10g status -h hedef ıp komutu ile sunucunun durum bilgisini

tnscmd10g ping -h hedef ıp komutu ile sunucunun ping bilgisini görüntüleyebiliyoruz.

2.32 METASPLOİT ARACI

Metasploit güvenlik testleri için geliştirilmiş olan, açık kaynak kodlu bir penetrasyon test aracıdır. Ruby dili ile kodlanmıştır pratik bir ara yüze ve kurallara sahiptir. İçerisinde 1000'in üzerinde exploit (zafiyet) barındırır. Metasploit içerinde, exploit ve diğer araçların kolay kullanımı için birçok parametre ve modül bulundurur

(Abdülaziz, 2017, s:9). Bu hack aracı aslında içerisinde çeşitli durum, sistem ve hedeflere yönelik zafiyetlerin ve kullanımlarını barındıran bir zafiyet kütüphanesidir.

ÜÇÜNCÜ BÖLÜM

ÖRNEK OLAYLAR

3.1 2001 OSMANLI BANKASININ HACKLENMESİ

Türkiye'ye internet bankacılığını getiren ilk bankalardan birisi olan Osmanlı Bankası'nın reklamlarında internet bankacılığı ve güvenli bankacılık hizmetleri tanıtılıyordu. Osmanlı Bankası, internet sitelerine giriş yapan müşterilerinin, kendi resimlerini görebilecekleri bir hizmet üzerinde çalışıyordu. Böylece internet bankacılığına giriş yapan müşteriler, kendi resimlerini gördüklerinde doğru internet sitesine girdiklerini anlayacaklar ve güven duyacaklardı. Osmanlı Bankasının yayınladığı bu reklamlar Türkiye'nin ilk hackerı olarak adlandırılan Tamer Şahin'in dikkatini çekmişti. Biraz internet bankacılığına olan merakından, birazda güvenliklerini denemek için bir internet bankacılığı hesabı açıp giriş yapan hacker Tamer Şahin bankanın bir sürü güvenlik açığı olduğunu fark etmiş ve bulduğu açıkları Osmanlı Bankası'na mail yolu ile bildirmiştir. Tamer Şahin'in aktardığına göre yetkililer açıklarının olmadığını güvenliklerinin üst düzey olduğunu yazan küçümseyici ifadeler içeren bir maille cevap vermişler. Fakat bir yandan da Tamer Şahin'in belirttiği güvenlik açıklarını kapatmaktan geri kalmamışlar. Bu cevaba kızan Tamer Şahin, tekrar Osmanlı Bankası'nın internet sayfasında açık arar ve bulur. Bulduğu güvenlik açığını kullanarak bankanın internet sitesini hacklar ve siteye *"Hello T.Ş. was here"* mesajını bırakır. İşlem yapmak için giren müşteriler bu mesajla karşılaşınca sitenin hacklendiğini anlarlar ve çevrelerine duyururlar. Haber çok hızlı yayılır, basında da yer edinir. Osmanlı Bankası bu olaydan sonra Tamer Şahin'den şikâyetçi olmuştur fakat yeterli delil elde edemedikleri için Tamer Şahin ceza almamıştır. Bir süre sonra da endişelenen müşterilerin mevduatlarını çekmeleri sonucunda banka batmıştır (Şahin, 2012, s:71-81).

Örneğimizde görmüş olduğunuz gibi Osmanlı Bankasını hackleyen hacker'ın ilk dalga etkisi olarak bankaya zararı sadece sitenin kullanım dışında kaldığı süre boyunca müşterilerin yapacakları bankacılık işlemlerinin büyüklüğü kadardır. Fakat sonuca baktığımızda bizim ardıl etki dediğimiz ekonomide dışsallıklar olarak geçen etki

sonucunda, Osmanlı Bankası batmıştır. Sonuç olarak bu örnekte de siber saldırının ardıl etkisi ilk etkisinden kat kat fazla olmuştur. Siber saldırıların ekonomik etkilerini doğru hesaplamanın ne kadar önemli olduğunu vurgulayan ibretlik bir örnektir. Yakın tarihimiz bu tür örneklerle doludur.

Siber saldırıların ekonomik etkilerinin hesaplanmasında.

Sektörlerin yıllık gelirlerini, bu sektörlerde bulunan firmaların yıllık firma başına ortalama siber saldırı maliyetini, bu firmaların sektörel ağırlıklarını ve sektörlerin ekonomideki ağırlıklarını göz önüne alınması gerekmektedir.

Her sektörün ve firmanın kendi ekosistemi içerisinde bir siber güvenlik politikası geliştirmesi gerekmektedir.

Firmalar:

- Tedarikçisi Oldukları Firmalar
- Kendi Tedarikçi Firmaları
- İş Yaptıkları Firmalar

Kapsayacak şekilde bir siber güvenlik politikası belirlemelidirler.

Yaptığımız araştırmalar doğrultusunda siber saldırı veya siber savaş olarak nitelendirilebilecek olayların herhangi birinin ardıl etki veya dolaylı etki olarak adlandırılan etkileri ilk etkisinden daha az olmamıştır. Bunun bir örneği yoktur. Burada saldırıların maliyetlerini hesaplarken düşülen hata, dışsallıkların göz ardı edilmesi ve ekonomik gerçeklerin iyi kavranamamış olmasıdır. Siber saldırılar hakkında istatistiki olarak çok fazla veri elimizde bulunmadığı için kapsamlı bir ekonometrik model kurma imkânımız bulunmamaktadır. Fakat siber saldırılar hakkında devletlerin dahi ellerinde yeterli derecede istatistiki veri mevcut değildir. İncelemiş olduğum birçok teknik kaynakta belirtildiği üzere, hükümetler bu konularda ağırdan hareket ediyorlar veya bu tür araştırmalarını gizli tutuyorlar. Veri bulmaktaki zorluğun daha iyi anlaşılması açısından uluslararası polis gücü olan Interpol'ün siber tehdit istihbaratı için 2018 yılının başlarında Kaspersky Lab ile antlaşma imzaladığının göz önünde bulundurulması gerekir. Bu yüzden örneğimizi, deyim yerindeyse kelebek etkisi olgusunun ekonometrik denklemlerde vücut bulmuş hali olan, çarpan etkisi üzerinden anlatmaya çalışacağız. Çarpan etkisinde marjinal tüketim eğilimi yani elde edin bir birim gelirin ne kadarının

harcanıp ne kadarının tasarruf edileceği üzerinden harcamaların etkileri hesaplanmaya çalışılacaktır.

Kurgulamış olduğumuz örnek aşağıdadır.

Örnek vermek gerekirse 1 milyon kişinin mevduatının olduğu bir banka düşünelim benim de bu bankanın müşterilerinden biri olduğumu farz edelim. Benim ve diğer 1 milyon kişinin bankada 1.000'er lira mevduatımız olduğunu varsayalım. Kuzey Koreli bir hacker grubu bu bankanın hesaplarını ele geçirip bu paralarla bitcoin almış olsun ve sonrasında da aldıkları bu bitcoini satarak izi sürülemeyecek şekilde parayı kendilerine aktarmış olsunlar.

Normal şartlar altında ben bu 1.000 liranın 700 TL'lik kısmını harcayıp 300 TL'lik kısmını tasarruf edecektim. Bu 700 TL ile yeni bir kitaplık almayı planlıyordum. Eğer bu para çalınmamış olsaydı ben 700 TL'ye kitaplık aldığımda mobilyacı da aynı şekilde benden kazandığı 700 TL'nin %30'unu tasarruf edip %70'ini harcayacaktı.

700x0.7=490 TL

Mobilyacı bu 490 TL'ye örneğin ayakkabı alacak olsun.

Ayakkabı aldığı ayakkabıcı da kazandığı 490 TL'nin aynı şekilde %30'unu tasarruf edip %70'ini harcayacaktır.

490x0.7=343 TL

Bu seri böyle sürüp gidecek.

Toplam etkiye bakıldığında

1000x[1/(1-MPC)] *MPC=Marjinal tüketim eğilimi.

1000x[1/(1-0.7)]

1000x[1/(0.3)]

1000x[0.33]=3,333 TL

Sonuç olarak eğer bu 1.000 lira benden çalınmamış olsaydı ekonomide 3.333 TL değerinde bir etkiye neden olacaktı. Fakat çalındığı için maliyet olarak kayıtlara geçen para sadece 1000 liradır. Eğer bu rakamı bütün mevduat sahipleri için hesaplarsak kayıtlara geçen çalınan para 1 milyar lira iken ekonomiye etkisi 3.3 milyar liradır.

(Saldırının bana olan etkisi 1.000 lira) + (Harcama yapamamam sonucunda ekonomiye olan etkisi 3.333) =4.333 TL (1.000/4.333/)x100=%23 ilk etki %77 ise dolaylı etkidir.

Gözden kaçırmamamız gereken bir diğer önemli nokta da tasarruf eğilimidir.

Ben normalde bu para çalınmamış olsa 1.000 Lira'nın %30 u olan 300 lirayı tasarruf edecektim ve bu para bankada duracaktı. Bankalarda bu parayla yatırımlar yapıp gelir elde edeceklerdi. Çalınan toplam meblağ açısından banka 300 milyon TL'lik bir mevduatı kullanabilecekken oluşan yeni durumda mevduat sahiplerine 1 milyar TL borçlanmıştır. Bankaların karşılık oranının ülkemizde %20 olduğunu düşünürsek banka elinde tutabileceği 300 milyon TL mevduatla 1.5 milyar TL kaydi para oluşturup yatırımlar yapabilirdi.

Ayrıca etki burada da sona ermiş değildir. Son durumda benden 1000 lira para çıktı fakat ben almayı düşündüğüm kitaplığı alamadım. Bu kitaplığı almak için gelecek aylarda tasarruf eğilimimi arttırmak zorunda kalacağım. Örneğin her 1000 liranın 700 lirasını harcıyorken artık 500 lirasını harcayıp 500 lirasını tasarruf ederek kitaplığı almaya çalışacağım. Bu durumu 1 milyon kişi için düşünürsek toplamda ekonomiye

(Fazladan tasarruf edilen 200 lira) x (1.milyon) = 200 Milyon Lira

Büyüklüğünde para daha uzun süre zarfında girecektir. Yani herkes almayı planladıkları şeyi alacak parayı tekrar biriktirene kadar bu para ekonomiye girmeyecektir. Faiz oranlara bağlı olarak ta bu denli bir paranın fazladan kullanım maliyetleri ortaya çıkacaktır.

Burada dikkat edilmesi gereken bir diğer hususta parayı benden çalan hackerların kendi ülkelerinde harcama yapmak için fazladan 1 milyar 'liraları oldu. Aynı şekilde onunda %30'luk tasarruf eğilimi %70 harcama eğilimi olduğunu varsayarsak siber saldırının toplam etkisi:

3.3x2=6.6 milyar TL'dir.

Bütün bu etkilere ilave olarak birde bu bankaya olan güven sarsıldığı için bir dışsal etki olarak kimse bu bankaya parasını yatırmayı düşünmeyecektir. Sonrasında gelişen süreçte bankaya hücum dediğimiz olay gerçekleşecek ve herkes bu bankadan parasını çekmek isteyecektir. Bunun sonucunda banka toplu halde mevduatları ödeyemeyeceği için batacak, banka çalışanları işsiz kalacak, bankanın kredi sağladığı birçok sektör de bundan etkilenecektir. Bu banka battığında örneğin 100 adet bankanın bulunduğu bir ülke

olduğunu varsayarsak bankacılık sektöründe artık 99 adet banka olacaktır. Ve bu bankaların bir rakipleri piyasadan çekildiği için faiz oranlarında %1'lik bir artışa gittiğini varsayalım. Bu durumda yatırımlar, tasarruflar ve bütün ekonomi etkilenecektir.

İlave bir etki olarak bu olayın meydana gelmesinden dolayı endişeye kapılan diğer bankalar siber güvenlik yatırımlarını arttıracaklardır. Normal şartlar altında yatırımlara harcayacakları paranın bir kısmını siber güvenlik yatırımlarına aktaracaklardır. Bunun sonucunda da ek güvenlik maliyetlerini müşterilere aktarmaya çalışacaklardır. Örnek vermek gerekirse bu olayın ardından siber güvenlik yatırımlarını arttıran 10 banka vadeli mevduatlara verdikleri faiz oranlarını %1 oranında düşürmüş olsun.

Sizin de bir yatırımcı olduğunuzu varsayalım. Böyle bir ortamda %1 fazla faiz almak için paranızı riske mi atardınız? Yoksa paranızı riske atmayıp %1 daha az faiz almak pahasına paranızı siber güvenlik yatırımlarını arttıran bankalara mı yatırırdınız?

İlk dalga etkisi 1 milyar lira olan bir siber saldırının ekonomiye etkisinin nerelere varabileceğini betimlemeye çalıştık. Fakat elbette gözden kaçırdığımız hususlar olacaktır. Siber saldırılar ya da siber savaşlar, savaş ekonomisinin bir konusudur. Ve savaş ekonomisinin doğasını yansıtırlar. Sonuç olarak etkileri de tıpkı bir yangın, doğal felaket veya savaş gibi ardıl olarak artarak devam eder. Örneğin bir yangında çoğu zaman bir evin yanmasının maliyeti göze çarpar fakat artan yangınlar ve bu yangınları söndürmek için harcanan iş gücü ve para hep geri planda kalır. Oysa bu tür ekonomik etkileri hesaplamak hayati öneme sahiptir. Bu tür etkiler iyi analiz edilmezse örneğin bir yangının 1000 liralık bir zarara yol açacağı bilinirken yangına müdahale yöntemi olarak helikopterle müdahale yöntemi seçilirse, yangının söndürme maliyeti yangının neden olacağı maliyetten daha fazla olur. Fakat nasıl ki bir savaşın, bir doğal felaketin ya da bir yangının çoğu zaman ardıl etkilerini ekonomik açıdan hesaplamak zor ise siber saldırılar içinde bu durum geçerlidir.

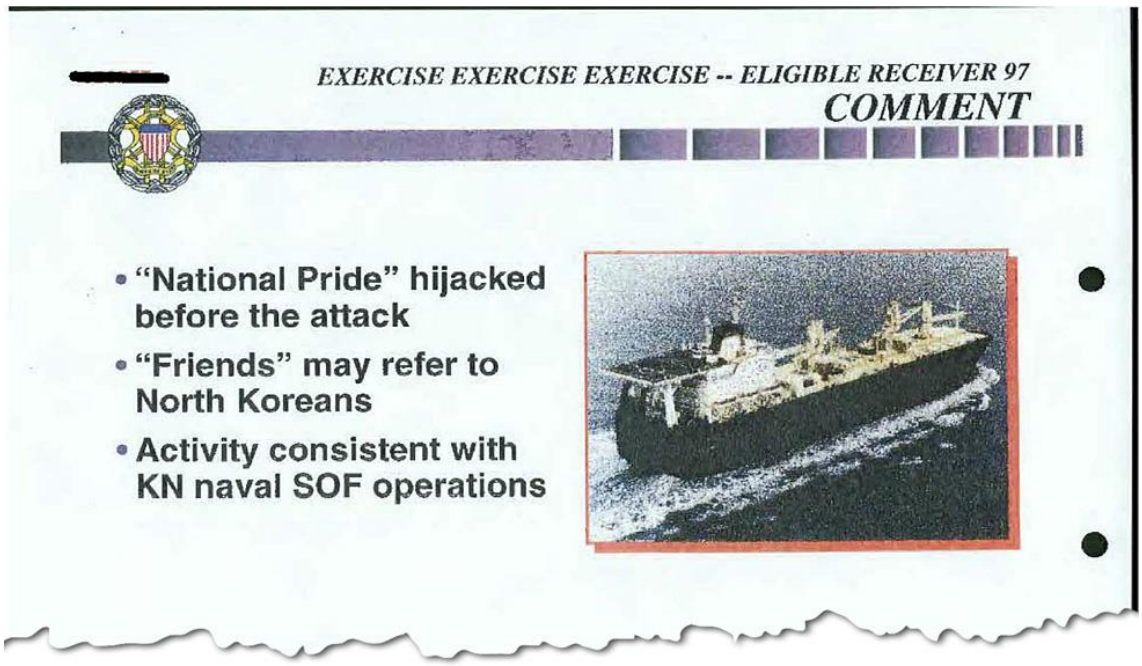
Siber saldırıların veya siber savaşların ekonomik etkilerinin hesaplanmasında yapılan hatalar veya eksiklikler ortadadır. Siber saldırıların etkilerinin gerçek etkilerine daha yakın olarak hesaplanabilmesi için, yukarıda anlatmış olduğumuz üzere çarpan etkisi, tasarruf etkisi, yatırım çarpanı, kamu harcama çarpanı gibi daha pek çok ekonomik etmen denkleme eklenmelidir. Bu tür hesaplamaların gerçeğe yakın olması için ekonomistler, siber güvenlik uzmanları, psikologlar, sigortacılık değerleme uzmanları,

yapay zekâ uzmanları ve daha pek çok disiplin bir araya gelerek ortak bir çalışma geliştirmelidirler. Nasıl ki devletler savaş teknolojileri ve savaş stratejileri geliştirirken bilimin her alanından yararlanıyorlarsa siber saldırıların ekonomik etkisini gerçeğe yakın olarak hesaplamak için de bilimin her alanından yararlanmak gerekir. En nihayetinde siber ortam ortaya çıkmış yeni bir savaş alanıdır ve savaşın doğasını yansıtmaktadır. Günümüzün rağbet gören konularından birisi de siber güvenlik sigortasıdır. Fakat incelemiş olduğum onca kurum raporu sonucunda, varmış olduğum kanı bu sektörün henüz emekleme evresinde olduğudur. Bununla beraber gelecek vadeden bir sektördür. Sigorta uzmanları, olası her kaza olayının ve yaşanan olay sonucunda değerleme yapılacak tekniklerin bulunduğu bir mevzuata sahiptirler. Aynı şekilde bilimin her alanından yararlanarak, her yönüyle siber saldırı ve savaşların olası etkilerinin ve gerçekleşebilecek olaylar sonucunda izlenecek prosedürlerin, hesaplama yöntemlerinin ve tekniklerinin ele alınıp bir yol haritası çıkarılması gerekmektedir.

Siber saldırıların hesaplanmasında izlenebilecek yöntemlere ek olarak yapay zekânın finansal kullanım alanları başlığı altında incelemiş olduğumuz tekniklerdir. Araştırmacılar, finansal analiz için geliştirdikleri yapay zekâ modellerinde veri olarak şirketlerin mali durumunu gösteren muhasebe bilgilerini kullanarak yüksek başarı oranıyla şirketlerin akıbetini tespit etmişlerdir. Benzer şekilde siber saldırıların gerçek etkilerinin hesaplanabilmesi için de saldırıya uğrayan hedefin bulunduğu sektör, uğradığı mali zararın büyüklüğü, bulunduğu ekonominin ekonometrik verileri, şirketin sektör içindeki büyüklüğü gibi bir takım verilerin etkileşimli olarak incelenmesi gerekmektedir. Bu verilere çeşitli bilimsel disiplinlerin geliştireceği teknikleri içeren veriler de ilave edildiğinde siber saldırıların etkisi gerçeğe daha yakın olarak hesaplanabilecektir.

Son olarak devam eden örnekleri, kurgu örnekte açıklamaya çalıştığımız dinamikleri göz önüne alarak değerlendiriniz.

3.2 1997 ELİGİBLE RECEVİER VAKASI



Şekil 18: ER97 Vakası

Kaynak:https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations

Eligible Recevier 97 "Uygun Alıcı 97" (ER97) olarak adlandırılan bir Savunma Bakanlığı siber güvenlik tatbikatıdır. Tehditlerin potansiyel kapsamını göstermek için saf siber faaliyetlerin ötesine geçen daha önce yapılmamış bir dizi sahte terör saldırısı, rehineye el koyma ve özel harekât saldırıları düzenledi. ABD ulusal güvenliği, son zamanlarda yayınlanan belgelere ve bugün George Washington Üniversitesi'ndeki Ulusal Güvenlik Arşivi tarafından yayınlanan Ulusal Güvenlik Ajansı (NSA) videosuna göre siber alanda yapılan saldırılarla şekillendi.

Clinton başkanlığında yürütülen ER97, ABD'nin siber uzaydaki tehditleri değerlendirilmesinde sık sık kritik bir olay olarak görülüyor. Tatbikat boyunca, piyasada satılan standart kullanıcılıların elde edebileceği donanım kullanan başlarında Donanma Kaptanı Michael SAYER'in bulunduğu bir NSA Kırmızı Takımı, sivil altyapı ağlarına erişim sağladı ve Savunma Bakanlığı ağlarına ciddi şekilde aşağılayıcı askeri komuta ve kontrol sistemleri noktasına erişmeyi etmeyi başardı. Savunan tarafta ise Pentagon çalışanlarının yanı sıra birde onlara yardımcı olmak üzere Mavi Takım bulunuyordu. Tatbikatın şok edici sonuçları doğrudan, ABD Siber Komutanlığı (USCYBERCOM)'un

kurulmasına yol açtı (*https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations*, 07.07.2019)

Eligible Receiver, 2003 yılında daha kapsamlı olarak Eligible Receiver 2003 olarak tekrarlanmıştır. Tüm bu tatbikatlar siber alandan gelebilecek tehlikelerin boyutlarını ve sistemlerin saldırılara karşı durumlarını ortaya koymuş ve atılması gereken adımlara ışık tutmuştur (Kaya, 2012:50). Günümüzde de bu tür tatbikatlara benzer organizasyonlar düzenlenmektedir. Örnek vermek gerekirse İstanbul'a kurulan 3. Havalimanı'nın lansmanında "Teknofest" organizasyonu düzenlenmiştir. Bu organizasyonun etkinliklerinden birisi de siber güvenlik testlerinin yüzlerce katılımcı etik hacker ve katılımcı hack grupları tarafından uygulanmasıdır. Etkinlik kapsamında yüzlerce siber güvenlik açığı tespit edilmiş ve açıklar kapatılmıştır. Bu tür organizasyonlar potansiyel riskleri önlemek açısından önemlidir.

3.3 1998 SOLAR SUNRİSE VAKASI

Şubat 1998'de ABD Savunma Bakanlığı ağı bir grup saldırıya maruz kalmıştır. Saldırı yöntemi olarak UNIX tabanlı işletim sistemi olan Solaris'teki bir açık kullanılmıştır. Saldırganlar önce sistemde bu açığın var olup olmadığını kontrol etmişler, mevcut olduğunu fark edince de bu açıktan faydalanıp sisteme, bilgi toplama maksatlı bir program yerleştirmişler ve daha sonra toplanan bilgileri almak için geri gelmişlerdir (Hildreth, 2001) (Kaya, 2012:51). 1-26 Şubat 1998 arasında gerçekleşen saldırılarda, saldırganlar aynı saldırı metodunu takip etmişlerdir:

1. Bu güvenlik açığının mevcut olup olmadığını tespit etmek için araştırma yapmak,
2. Güvenlik açığından yararlanmak,
3. Veri toplamak için bir program kullanmak (sniffer)
4. Toplanan verileri almak için daha sonra geri dönmek

(https://www.globalsecurity.org/military/ops/solar-sunrise.htm, 07.07.2019).

3.4 1999 KOSOVA VAKASI

NATO uçakları Kosova Savaşı esnasında Sırbistan'ı bombalamaya başlayınca, "Black Hand" gibi Sırp yanlısı ve Batı karşıtı hacker grupları NATO'nun internet altyapısına saldırmaya başladı. Siber saldırıların, Yugoslavya Federal Cumhuriyeti'nin askeri kuvveti için gerçekleştirilip gerçekleştirilmediği tespit edilemese de, NATO'nun askeri operasyonlarını bozmayı hedeflediği ortadadır. "Black Hand" hacker grubu ismini, 1'inci Dünya Savaşı'nın başlamasına sebep olan Pan-Slav gizli bir topluluktan almıştır. Savaş sırasında "Black Hand" hacker grubunun NATO'ya ait en önemli bilgisayarları ele geçirdiği ve bilgisayarlar üzerindeki tüm verileri sildiği iddia edilmiştir (Ronfeldt, & Arquilla, 2001) (Ada & Çakır, 2017:638).

NATO, Kosova Savaşı'nda amacına ulaşmış gibi görünse de siber saldırılar karşısında yetersiz kalmıştır. NATO'ya yapılan saldırıda, web sitelerine bırakılan mesajlar, saldırganların kim olduklarını; olayın evveliyatına bakıldığında ise neden bu saldırıyı yaptıklarını açıkça göstermektedir. Kosova'da maruz kalınan siber saldırılar NATO'yu yeni bir stratejik doküman hazırlamaya zorlamıştır. Bu dokümanda siber tehditlere çok az değinilmiş olsa da NATO'nun siber güvenlik alanında ilk adımı bu şekilde atılmıştır (Ada & Çakır, 2017:638).

NATO literatürene siber güvenlik kavramını sokan bu tür saldırı örneklerinin stratejiden yoksun olması askeri açıdan çok büyük problemlere neden olamayabilir. Fakat dışsallıklar açısından bakıldığında NATO ülkelerinde veya NATO'ya karşı kurulan birliklerde NATO'nun imajının zedelenmesine ve kırık cam etkisi yaratarak yeni saldırılara neden olabilmektedir. Bu tür imkânları keşfeden NATO karşıtı devletler daha stratejik hareket ederek planlı bir şekilde adeta bir kırık cam olan NATO'nun siber güvenlik konusundaki bu eksikliklerini kullanarak organizasyon hakkında ciddi veriler elde etmeyi deneyeceklerdir. Söz konusu savaş, ordu veya savaş ekonomisi olduğunda elde edilebilecek her türlü gizli bilgi hayati öneme sahip olabilmektedir. Savaş planları, tatbikat ve savaş düzeni, envanter, asker sayısı ve daha pek çok önemli bilgi. Bu tür bilgilere ekonomik bir değer biçmek oldukça güç olmakla beraber en hafif haliyle bu tür bilgileri bir askeri casustan alabilmek için ciddi bir yatırım yapılması gerektiği söylenebilir. Bu tür bilgilerin açığa çıkmasının savaş veya savunma sistemlerinin işlerliğini tehlikeye sokması açısından da önemli bir ekonomik etkisinin olduğunu

söylemek mümkündür. Çalınan bilginin ne olduğuna bağlı olarak bu zarar veya düşman açısından elde edilen fayda değişmektedir. Örnek vermek gerekirse bu tür askeri tesislerden çalınan bir radar tasarımı bilgisi, ilk dalga zarar açısından en az hava kontrol ve gözetleme sistemlerinin maliyeti kadardır. Çünkü artık bu sistemler düşman tarafından elde edilen bilgiler sayesinde tersine mühendislik yöntemleri kullanılarak karıştırma dediğimiz radarların işlevini yerine getirememesine veya radarların yanıltılmasına neden olacaktır. İkinci dalga ekonomik etki olarak ta bu radar sistemlerine güvenerek kurulan savunma hattı çökecek ve en az bu hattaki bütün askeri tesis ve ekipmanların maliyeti kadar, ardıl bir ekonomik etkiye neden olacaktır. Nitekim aşağıdaki Moonligt Maze vakasında ABD'nin savunma bakanlığından bu tür kritik bilgiler çalınmıştır.

3.5 1998 MOONLİGHT MAZE VAKASI

Şekil 19: Moonlight Maze
Kaynak: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf , 07.07.2019

Moonlight Maze operasyonu olarak bilinen ve Mart 1998'de başlayan operasyon ile ABD'nin Pentagon, NASA, ABD Enerji Bakanlığı ve üniversitelere ait araştırma ve geliştirme sırları, askeri tesislerin haritaları, askeri yapılandırmaları ve askeri donanım tasarımlarını içeren birçok gizli bilgi çalınmıştır (Kara, 2013:42).

Bu saldırıyı temelde diğerlerinden ayıran nokta rastgele olmaktan öte organize bir şekilde gerçekleştirilmiş olmasıdır. Saldırıda tasnif dışı bilgilerin yer aldığı bilgisayarlara erişildiği rapor edilmiş olsa da genel anlamda sistemlerde hassas bilgilerin yer alması ve bu saldırıların göstermiş olduğu potansiyel tehlike çok önemlidir. Saldırılarla ilgili yapılan iz sürme sonucunda bu saldırıların Moskova'nın 20 mil dışında yer alan ve Rusya Bilimler Akademisi ile sıkı bağları olan bir servis sağlayıcı üzerinden gerçekleştirildiği belirtilmiştir (Cordesman, 2002)'ye atfen (Kaya, 2012:52). ABD'nin milyonlarca dolar harcayarak ve yıllarca çalışarak elde ettiği deneyim, bir operasyonla el değiştirmiş oldu. Ekonomik açıdan hesaplanamayacak düzeyde bir zarar söz konusudur. İlk dalga etki olarak yaşanan yüklü miktarda veri ihlali sonucunda ABD bütün askeri yapılanmasını yeniden tasarlamak zorunda kalacaktır. Çünkü artık bütün karargâh koordinatları, askeri tesislerinin yerleri ve stratejileri düşmanın eline geçmiştir. Yıllarca süren çalışmaların sonucu olan araştırmalar, tasarımlar ve çalınan birçok gizli bilginin ekonomik değer açısından yol açtığı etki en azından milyarlarca dolar olmalıdır. Ayrıca elde edilen bilgi sonucunda Rusya'nın ABD ye karşı elde ettiği bilgi üstünlüğü asimetrik bilgi durumuna yol açacağı için Rusya savunma yatırımlarını daha isabetli yapacaktır. Ve savunma endişesiyle gereksiz yatırımlar yapmak zorunda kalmayarak kaynaklarını daha verimli projelere aktaracaktır. Bütün bu sonuçlar daha fazlası bu saldırının dışsallıkları arasındadır.

3.6 2001 AVUSTRALYA ATIK SİSTEMİ SCADA VAKASI

Yazılım geliştirme ekibinin eski bir çalışanı, şirketin Park Yerinden WIFI bağlantısını kullanarak Queensland atık su arıtma tesisini kontrol eden SCADA sistemini defalarca kez hackledi. Ardından yakınlardaki nehirlere ve parklara yaklaşık 264.000 galon ham kanalizasyon salıverdi (https://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/ 08.07.2019). Bu olayda ilk dalga ekonomik etki, atık su arıtma sisteminin çalışmadığı süre boyunca, atık sisteminin çalışması için harcanan para kadardır. Çünkü bu süre zarfında sistem çalışmamış ve sistemin çalışması için harcanan para boşa gitmiştir. Ardıl etkileri veya bu olayın neden olduğu dışsallıklar ise bu atık su arıtma tesisinin çalışmaması sonucunda yakınlardaki nehirlere atık su boşaltması sonucunda nehirler kirlenmiştir. Nehirlerin kirlenmesi sonucunda oradaki ekosistem

tehlikeye girmiştir. Tekrardan nehirlerin temizlenmesi ve eski haline gelmesi zaman alacağı gibi bu tür çevre düzenlemeleri için firmalar, belediyeler ve ülkeler bir hayli para harcamaktadırlar. Bir diğer muhtemel etki olarak ta burada balıkçılık yapan bireyler bir süre balık avlayamayacaktır ve gelirlerinde bir azalma meydana gelecektir. Bu nehir kenarlarına piknik yapmak için gelen yerli ve yabancı turistler nehirler eski haline gelene kadar buralara uğramayacaklardır. Bunun sonucunda da turizm gelirlerinde bir miktar azalma meydana gelecektir. Son olarak her siber saldırıdan sonra olduğu gibi atık su arıtma tesisi siber güvenlik yatırımlarını arttırmak zorunda kalacaktır. Ve bu ekstra güvenlik önlemleri için harcadıkları para yüzünden kârlılık oranları düşecektir.

3.7 2000 İSRAİL-HİZBULLAH VAKASI

Filistin- İsrail çatışmasına 'internet savaşı' eklendi. Dünyanın dört bir köşesinden yapılan 'saldırılarla İsrail Parlamentosu, Dışişleri Bakanlığı, silahlı kuvvetler ve başbakanlık siteleri çökertildi. İsrail tam bir aydır sürdürdükleri ve 142 kişinin ölümüyle sonuçlanan taşlı silahlı çatışmalarını, internet cephesine de taşıdı. Her iki taraftan bilgisayar korsanları karşılıklı olarak birbirlerinin internet sitelerini sabote etmeye çalışınca İsrail ile Filistin arasındaki gerilim "siber savaşa" dönüştü.

Elektronik posta ile kilitlediler

AP haber ajansına göre siber savaşın fitilini, Lübnanlı Hizbullah örgütünün sitesine saldıran bir grup İsrailli genç ateşledi. Hizbullah'tan yapılan açıklamalarda da, örgütün çatışmaların başlamasının ardından ekim ayı başında üç İsrail askerini kaçırmasından bu yana iki kez sitelerinin çökertildiği doğrulandı. Ancak dünyanın dört bir yanındaki İslamcı gruplar misilleme olarak İsrail parlamentosu ve Dışişleri Bakanlığı'nın internetteki sitesini elektronik posta bombardımanına tutup çalışamaz hale getirdi. Söz konusu saldırıların Suudi Arabistan'daki bilgisayar korsanları tarafından gerçekleştirildiği sanılıyor. İsrail ordusu ve Başbakan Ehud Barak'ın ofisinin de saldırılardan nasibini alması üzerine savaş iyice kızıştı. Bir İsrail sitesi, aşırı dinci Hamas ve Hizbullah'ı hedef göstererek bilgisayar korsanlarına "saldırın ve yok edin" çağrısı yaptı.

Özel saldırı programları

İsrail Dışişleri yetkilileri birçok İslamcı örgütün kendi sitelerinde "İsrail'e ait internet sitelerine saldırması" çağrısında bulunduğunu hatta bazı bilgisayar

*programlarıyla her kullanıcıya yüzlerce elektronik posta gönderme imkânı sağladığını belirtti. Geçen yıl da bir İsrailli genç "www.iraq.com" adlı Irak sitesine bulaştırdığı virüsle siteyi çökerterek şöhrete kavuşmuştu (*http://www.milliyet.com.tr/dunya/siber-intifada-5335183, 8.7.2019*).*

Bu olayda ilk dalga etki olarak İsrail hükümetinin online hizmetlerini sunamaması sonucunda aksayan işler kadar bir etki ortaya çıkacaktır. Fakat dışsallıklar açısından bakıldığında bir devletin resmi kurumlarının internet sitelerinin hacklenmesi, hacklenen resmi sitelere giren vatandaşların hackerların antipropaganda yazılarını gördüklerinde devlete olan güvenlerini sarsacaktır. Devlet kurumu olarak özellikle istihbarat servislerinin internet siteleri pek çok açıdan kritik öneme sahiptir. En temel etki olarak bir devletin istihbarat birimlerinin resmi kurum sitelerinin hacklenmesi o istihbarat servisine karşı olan güveni sarsacaktır. Ayrıca siteyi ele geçiren hackerların ne tür bilgilere erişebildiklerini tam olarak bilmek mümkün olmadığı için istihbarat servisinin kadrolarında veya birimlerinde değişiklik yapmak zorunlu hale gelebilecektir. Bu tür kritik kurum sitelerinin hacklenmesinin doğurduğu bir diğer etki de normal şartlar altında istihbarat servisine düşman cephesinden bilgi vermeyi düşünebilecek potansiyel işbirlikçilerin deşifre olmaktan korkarak bilgi vermeye yanaşmamasına neden olacaktır. Buna benzer bir olay Aslan Neferler Tim isimli hacking grubunun Ermenistan istihbarat servisinin internet sitelerini hackleyerek Ermenistan istihbarat ajanlarının kimliklerini ele geçirip MİT'e göndermeleriyle yaşanmıştır. Ermenistan ajanları verilen bilgiler sayesinde yakalanmışlardır. Bir diğer açıdan siteyi hackleyen hackerlar normal şartlar altında yapamayacakları, milyon dolarlar değerinde dünya çapında reklam yapmış olmaktadırlar. Son olarak bütün bu saldırıların kurumun siber güvenliğini sorgulatacaktır ve ekstra siber güvenlik yatırımları yapmaya itecektir.

3.8 2001 CODE RED VAKASI

İlk defa Temmuz 2001'de ortaya çıkan Code Red solucanı ABD'de Microsoft'un IIS Web sunucularında bulunan bir güvenlik açığından faydalanarak yaklaşık olarak 300.000 bilgisayarı etkilemiştir. Solucan ayın 1 – 19 arasında kendisini çoğaltacak, 20 – 27 arasında belirli bir siteye Hizmet Dışı Bırakma (DOS) saldırısı gerçekleştirecek ve 27'sinden ay sonuna kadar da bilgisayarda sessiz bir şekilde uyuyacak şekilde

programlanmıştır. Code Red Solucanı'nın ilk türleri belirli tarihlerde Beyaz Saray'a Hizmet Dışı Bırakma saldırısı düzenleyecek şekilde programlanmıştır. Beyaz Saray'ın sistemi titizlikle korunsa da, diğer sitelerin hizmet veremez hale getirilip ana sayfalarının "Çinliler Tarafından Hacklendi" mesajı ile değiştirilmesinin önüne geçememiştir (http://www.pbs.org/wgbh/-pages/frontline/shows/cyberwar/warnings/) (Kaya, 2012:54).

Bu saldırıda, virüs etkilenen 300 bin bilgisayarın kullanıcıları tarafından tam verimle kullanılamamasına neden olmuştur. Ayrıca bulaştığı bilgisayarların bağlı olduğu ağları kullanarak resmi kurum sitelerine atak gerçekleştirmesi de 300 bin kullanıcının internet ağlarında verimsizliğe neden olacaktır. Örneğin 24mpbs (saniye başına indirilebilecek megabit) hızında çalışan bir ağın 12mpbs ile çalışmasına neden olması durumunda virüsün ağı kullandığı süre boyunca kullanıcıların internet hizmetleri için ödedikleri ücretlerin yarısı kadar bir zarara yol açacaktır. Gene saldırıya uğrayan sitelerin sağladıkları servislerin aksaması da ilk dalga etkisi olarak karşımıza çıkacaktır. Fakat ardıl etki olarak virüsten etkilenen 300 bin kullanıcı başta olmak üzere bu olayın gündeme oturması sonucunda tehdit algısı geliştiren yüzbinlerce, belki milyonlarca kullanıcının siber güvenlik paketleri satın almasına neden olacaktır. Ayrıca Microsoft firmasına olan güven de sarsılacağı için firma açısından da ayrıca olumsuz yönde dışsallıklara neden olarak satışlarının düşmesine neden olacaktır.

3.9 2001 ÇİN - ABD SİBER SAVAŞI

2001 yılının Nisan ayında bir Çin savaş uçağıyla ABD gözetleme uçağının çarpışması sonrasında bazı Çinli hacker grupları (Honker Union of China ve Chinese Red Guest Network Security Technology Allience gibi) ABD'ye karşı yoğun ve uzun süreli siber saldırılar düzenlemişlerdir. Çinli hacker grupları Beyaz Saray, Amerikan Enerji Bakanlığı ve Amerikan Hava Kuvvetleri'nin de içinde bulunduğu yaklaşık 1200 siteye DDoS saldırıları düzenlemişlerdir (Vatis, 2001:8). ABD'yi hedef alan siber saldırıların kaynağının belli olmasına rağmen, Çin hükümeti bu saldırılara karşı bir yaptırım uygulamamıştır. Bu saldırıların Çin hükümeti tarafından desteklendiği ya da en azından görmezden gelindiği açıktır (Gürkaynak & İren, 2011:271).

Bu saldırılar süresince ulaşılamayan 1200 internet sitesinin hizmet verememesi sonucunda işler aksayacaktır. Ve aksayan işler sonucunda bu sitelerin ekonomi ile entegrasyonuna bağlı olarak bir ilk dalga etkisine neden olmuşlardır. Saldırıların gerçek zararını hesaplamak için erişime kapatılan sitelerin ne tür siteler olduğu, ortalama günlük bu internet siterleri üzerinden ne tür hizmetlerin verildiği dolayısıyla aksayan hizmetlerin neler olduğu araştırılmalıdır. Örnek vermek gerekirse bu internet siteleri arasında online alışveriş siteleri bulunması durumunda erişime kapatıldığı süre zarfında ziyaretçiler bu sitelerden alışveriş yapamayacaklardır. Günlük ortalama 5.000$ alışveriş yapılan toplamda 100 site erişime kapatılmış olsa dahi olsa 5.000x100 = 0.5 milyon$ sadece bu yüz siteye verilen ilk dalga etkisi zararıdır. Kaldı ki bu rakamlar çarpan etkisi ve dışsallıklar yoluyla gitgide katlanarak artacaktır. Bu tür internet sitelerin erişemeyen müşteriler başka internet sitelerini tercih edecekler ve erişemedikleri siteler hakkında güvensizlik duyarak güvenlik algıları sarsılacaktır. Kimse hacklenen bir alışveriş sitesinden kredi kartıyla alışveriş yapmak istemez. Belki siteyi hackleyen hackerların erişimi sadece yüzeyseldir. Sadece site ara yüzüyle sınırlıdır. Belki internet sitesinin veri tabanına erişim sağlayamamışlardır. Fakat bunu kimse bilemez ve kimse bu riski alıp kredi kartı bilgilerini güvenli olmayan mecralarda kullanmaz. Dolayısıyla bu tür görünürde basit bir hacking olayının bile milyonlarca dolarlık dışsallık etkisi söz konusudur.

3.10 2003 TİTAN RAİN VAKASI

2003 yılında ABD'nin uğradığı Titan Rain saldırısında, NASA'dan, ABD askeri kurumlarından ve firmalarından bilgi çalınmıştır. Bu olay 1998 yılında yaşanan Ay Işı Labirenti operasyonunun benzeridir. Yapılan araştırmalar sonucunda Titan Rain saldırısının Çin kaynaklı olduğu anlaşılmıştır (Kara, 2013:29). Yetkililer ABD'nin askeri ağından 10 ila 20 terabayt arasında veri çalındığını belirtmişlerdir. Daha öncesinde 1998 yılında yaşanan bir benzer saldırı olan Moonlight Maze (Ay Işığı Labirenti) olayı bir kırık cam etkisi ile Titan Rain olayını doğurmuştur. Moonligt Maze olayıyla ABD'nin siber güvenlik zafiyeti olduğunu öğrenen taraflardan biri olan Çin'de belli ki bu durumu istismar ederek kendi çıkarları açısından önemli bir kazanım elde etmek istemiştir. Moonligt Maze vakasının üzerinden geçen 5 yıla rağmen belli ki ABD siber güvenlik

konusunda hala önemli zafiyetlere sahiptir. Bu tür büyük çaplı veri ihlallerinin sık sık tekrar etmesinin getirdiği ekonomik zararın yanında tekrarlanmasından kaynaklanan güvensizliğin etkisi de giderek artacaktır. Bunlara ilave olarak siber güvenlik konusunda ilk veri ihlalinden bu zamana kadar geçen süre zarfında emek harcayanlar da artık siber güvenliğin sağlanabileceğinden şüphe edecekler ve isteksiz çalışacaklardır. Aynı durum tekrar tekrar geliştirdikleri stratejiler çalınan askeri kurumlar ve araştırmaları çalınan araştırma kurumları için de geçerlidir. Onlar da sürekli emeklerinin boşa gittiğini düşünerek isteksiz çalışacaklardır. Bütün bunların ve halkın gözünde itibar zedelenmesinin ABD'nin iç ve dış ilişkilerine vereceği zararın ekonomik boyutunu hesaplamak zordur. Bununla birlikte Çin ve Rusya gibi bu tür saldırıları gerçekleştiren ülkeler ABD ile çıkarları çatışan ülkelerin dikkatini çekecektir ve endüstriyel casusluk konusunda Çin ve Rusya ile işbirliğine gideceklerdir. Diğer bir deyişle Çin ve Rusya'nın çaldıkları verileri pazarlayarak gelir elde etmeleri de söz konusudur. Örnek vermek gerekirse Kuzey Kore ve İran gibi ABD karşıtı strateji geliştiren ülkeler bu tür verilere önemli meblağlar vermeye gönüllü olacaklardır.

3.11 2003 ABD VE KANADA ELEKTRİK KESİNTİSİ

14 Ağustos 2003 tarihinde Kanada'nın Ontario eyaleti ve ABD'nin Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut ve New Jersey eyaletlerinde elektrik kesintisi meydana gelmiştir. 50 milyon insanın etkilendiği kesinti ABD tarihinin en büyük elektrik kesintisi olma özelliğini taşımaktadır. Ontario eyaletinde bir haftadan fazla süren kesinti, ABD eyaletlerinde 4 gün sürmüştür. Bu süreçte kesintinin yalnızca ABD'ye maliyetinin 4 ila 10 milyar dolar olduğu belirtilmektedir. Ontario'da ise üretimin aksamasından kaynaklanan zararın yaklaşık 2,3 milyar Kanada doları olduğu tahmin edilmektedir (http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf),(MERAL, 2015:82). Elektrik santralinde meydana gelen çökmeden dolayı gerçekleşen bu olayda bahsedilen ilk dalga ekonomik etki olan en az 4 milyar dolar ABD'ye olan etkisi ve 2.3 milyar Kanada doları olan Kanada'ya etkisidir. Dışsallık bakımından ABD'nin dünyanın en büyük ekonomisi olduğu göz önüne alındığında 4 gün boyunca elektriksiz kalınması sonucunda ABD'nin dış ticaretinde gerçekleşen

aksamaların ABD ile ticaret yapan ülkelere olan etkisi de bir diğer dışsallıktır. Bunun yanı sıra bu tür elektrik kesintileri için alınacak önlemler bireysel ve devlet bazında ekstra harcamalara yol açacaktır. Belki de bir daha yıllarca yaşanmayacak elektrik kesintisi için önlem olarak firmalar jeneratör alacaklardır bireyler de aynı şekilde bu tür önlemlere gideceklerdir. Kamu binaları ve kurumları da benzer önlemler alacaklardır. Sonuç olarak gene milyonlarca dolar daha iyi değerlendirilebilecekken ihtiyat amaçlı olarak bu tür atıl yatırımlara aktarılacaktır.

3.12 2003 BATMAN HİDROELEKTRİK SANTRALİNİN ŞİFRELENMESİ

2003 yılında Batman Barajı hidroelektrik Santralı'nın yapımını üstlenen Alman Noel Şirketi, 1 milyon dolar alacağını tahsil edemediği gerekçesiyle şirketin bilgisayarlarını şifre ile kilitleyip, kenti terk etti. Şifreleme nedeniyle santralin üç ünitesinde de enerji üretimi durdu. Bilgisayarların şifrelenerek kilitlenmesi nedeniyle Batman Barajı'nda enerji üretimi yapılamadığını söyleyen DSİ yetkilileri, bu nedenle Batman'ın bazı ilçeleri ile Şırnak ve Cizre'ye kesintili olarak elektrik verebildiklerini belirttiler. Barajın yeniden elektrik üretimine başlaması için şifreyi çözmek üzere Türkiye Elektromekanik Sanayi uzmanları da yoğun çalışmalarını sürdürüyor. Uzmanlar bir yandan şifreyi çözmeye, bir yandan da Alman firması yetkililerine ulaşmaya çalışıyor (http://www.milliyet.com.tr/ekonomi/batman-baraji-sifrelendi-5176871, 8.7.2019). Bu örnek bireysel olsun, kamu kurumları ve sanayi kuruluşları açısından olsun, PLC, SCADA ve işletim sistemleri gibi siber çevre birimlerinin yerliliğinin önemini göstermektedir. İleride anlatacağımız Stuxnet vakasında olduğu gibi burada da çevre birimlerinin kaynak kod düzeyinde yerliliği sağlanmadıkça kontrolün tam olarak elde tutulamadığı görülmektedir. Bu örnekte anlatılan kriz ne kadar sürdü ne kadar süre zarfında çözüme kavuşturulduğu bilinmemekle beraber ilk dalga etkisi bu elektrik kesintisinin etkilediği yerleşim birimlerinde tüketilen elektrik enerjisinin parasal değeri kadardır. Sonrasında bu maliyete bu süre zarfında tüketilen elektrik enerjisi ile gerçekleştirilebilecek üretimin maliyeti eklenmeli. Ve bu girdilerin bölgesel ekonomiye etkilerinin yanı sıra diğer bölgelerle olan ticarete etkileri de ayrıca hesaba katılmalı.

3.13 2003 OHİO NÜKLEER TESİS VAKASI

Slammer Solucanı Ohio Nükleer Tesisi ’ne kendilerinin bağlı olduğu grup şirketin bir danışmanının bilgisayarından bulaşmıştır. Solucan tesisin ana ağını ve kontrol sistemleri ağını etkilemiştir. Personel 4 saat 50 dakika boyunca, reaktör çekirdeğindeki soğutucu sistemleri, sıcaklık algılayıcılar ve radyasyon dedektörlerinden gelen hassas verileri gösteren Güvenlik Parametreleri Görüntüleme Sistemlerine ağdan erişilememiştir (Akar, 2015:3).

Görünürde üretimde bir aksama yaşanmamış ve ekonomik etki oluşmamıştır. Fakat bu tür bir sorunu çözmek için nükleer santrali bir süreliğine durdurarak işleri yoluna koyana kadar çalıştırmamak en akılcı çözüm olacaktır. Çünkü nükleer santrallerde bulunan radyoaktif maddelerin yaydıkları ısı, soğutularak belirli bir düzeyde tutulmazsa nükleer santralde patlama meydana gelebilir. Göstergelerden emin olunamadığı böyle bir durumun geç fark edilmesi veya fark edilememesi de bir patlamayla sonuçlanabilirdi. Santral elektrik üretimini durdurmamışsa dahi sistemleri normale dönene kadar her kontrol manuel olarak yapılacaktır ve buda üretimde verimsizlik olarak dönecektir. Ardıl ekonomik etki olarak ta siber güvenlik açısından zafiyet barındıran bu tesiste bu olaydan sonra bir dizi güvenlik önlemi alınarak siber güvenlik yatırımları yapılacaktır. Buna ek olarak bulaşan virüsün bir şirket çalışanının bilgisayarından bulaşmış olması da nükleer santralde ve şirketteki çalışanların siber güvenlik konusunda eğitilmesini gerektirecektir. Eğitim için düzenlenecek etkinliklerin masrafları da bu olayın dışsal etkileridir. Ve bu olaydan sonra şirkete dışarıdan bilgisayar sokulmasının yasaklanması gibi bir dizi sıkı güvenlik önlemi de alınacaktır. Ne kadar çok önlem o kadar çok güvenlik demektir fakat aynı zamanda ne kadar çok önlem alınırsa bir o kadar da çalışma esnekliği azalacaktır. Çalışanların kişisel bilgisayarlarına anti virüs ve güvenlik duvarı yazılımları alınmasına kadar bir sürü dışsal etkiye neden olacaktır.

3.14 2003 ADOBE FİRMASINA SİBER SALDIRI

Yazılım şirketi Adobe, 38 milyon civarında aktif kullanıcısının şifrelerinin ve kullanıcı adlarının çalındığını duyurdu. Adobe'den yapılan açıklamada, yakın bir süre önce düzenlenen siber saldırıda, sanılandan çok daha fazla müşterinin etkilendiğinin

ortaya çıktığı belirtildi. Şirket, şu anda yaklaşık 38 milyon aktif kullanıcının şifrelerinin ve kullanıcı adlarının çalındığına inanıldığını, internet korsanlarının aynı zamanda, iki yıldır veya daha uzun süredir kullanılmayan, sayısı belirsiz hesabın ayrıntılarına eriştiğini bildirdi. Siber saldırıda, popüler görüntü-düzenleme programı Photoshop'un kaynak kodunun bölümlerinin de çalındığı kaydedildi. Daha önce siber saldırıdan 2,9 milyon hesabın etkilendiğini açıklayan Abode, Acrobat PDF belge düzenleme yazılımının ve ColdFusion internet uygulamasının kaynak koduna yasadışı yollardan erişildiğini bildirmişti. Korsanların eriştiği bilgi, Adobe'nin yazılım çalışmalarını ne şekilde yürüttüğünün incelenmesini ve tekniklerinin kopyalanmasını sağlayabilir(http://www.hurriyet.com.tr/ekonomi/38-milyon-kisinin-sifresi-calindi-25011008 , 28.06.2019). Bu siber saldırının ekonomik etkileri saldırıda elde edilen kullanıcı bilgilerinin ne şekilde kullanılacağına bağlı olarak değişecektir.

3.15 2003 TARGET FİRMASINA SALDIRI

ABD'de mağazalarını tercih eden 40 milyon kişinin banka ve kredi kartı bilgilerinin çalındığını açıklayan perakende devi Target, yapılan soruşturmanın, mağdur müşteri sayısının aslında 70 milyon olduğunu, çalınan veriler arasında, adres, telefon ve elektronik posta gibi kişisel bilgilerin de yer aldığını ortaya çıkardığını açıkladı.

Target üst yöneticisi Gregg Steinha, gazetecilere, ABD'nin en büyük veri hırsızlıklarından biriyle ilgili açıklamada bulundu. Soruşturmanın, mağdur müşteri sayısının 70 milyon olduğunu ortaya koyduğunu belirten Steinha, çalınan veriler arasında kişisel adres ve telefon bilgilerinin de yer aldığını söyledi. Yeni bir hırsızlığın söz konusu olmadığının altını çizen Steinha, gelişmelerden üzgün olduğunu ifade ederek, durumu "sinir bozucu" olarak niteledi.

ABD'nin en yoğun alışveriş döneminde 27 Kasım ile 15 Aralık arasında Target'in sistemine giren hırsız, müşterilere ait bilgileri ele geçirmişti. Milyonlarca kişinin verilerinin çalınması, Target müşterileri arasında paniğe neden olmuştu(https://www.trthaber.com/haber/dunya/70-milyon-kisinin-banka-ve-kredi-karti-bilgileri-calindi-114896.html , 20.06.2019).

Bu örnekte ve ileride göreceğiniz Cathay Pasific örneğinde görüldüğü üzere firmalar ve hükümetler siber saldırıların etkilerini olduğundan daha az göstermeye veya saklamaya meyillidirler.

3.16 2006 WİKİLEAKS, ANONYMOUS VE ASSANGE

Şekil 20: Jullian Paul ASSANGE, Wikileaks ve Anonymous

Kaynak:https://misesuk.org/2013/01/29/the-new-fourth-estate-anonymous-wikileaks-and-archy/

2006 yılında "Biz Hükümetleri Açarız!" sloganıyla yayınlanmaya başlayan kurucusu ünlü Hacktivist Jullian Paul ASSANGE olan internet sitesidir. Yayına başladıktan bir yıl sonra ellerinde 1,2 milyon sızıntı belge olduğunu ilan etmişlerdir (Ertem & Uçkan, 2011:23). Irak operasyonunda görev yapmış ABD kıdemli eri Bradley Manning, 1966-2010 tarihleri arasında ABD Dış İşleri Bakanlığınca yapılan gizli yazışmaları, ordu veri tabanından indirdiği doküman ve görüntüleri, Wikileaks sitesine sızdırmıştır (Kara, 2013:17). Sızdırılan görüntülerde savaş suçları işleyen ABD askerleri bütün dünyada yankı uyandırmıştır. Bu tür sızıntılardan sonra Wikileaks bir akıma dönüşmüştür ve Wikileaks gazeteciliği denilen bu akımda devletlerin en mahrem sırları açıkça yayınlanmaya başlanmıştır. Adrian Lamo isminde eski bir hackerın belgeleri sızdıranın Er Bradley Manning olduğunu ihbar etmesi üzerine 2010 Mayıs ayında Er Manning casusluk suçlamasıyla Irak'ta tutuklanarak Quantico'daki deniz kuvvetleri hapishanesine gönderildi. İstifasına neden olan bir olaydan sonra, Dışişleri Bakanlığı sözcüsü Phillip J. Crowley, bulunduğu hapishanede Manning'e kötü muamele yapıldığını ve bu yapılanları kınadığını belirten açıklamalarda bulundu. Durumun vahameti yetkililerce de itiraf edildikten sonra Anonymous harekete geçerek Bradical Operasyonu

ismiyle anılacak bir dizi saldırı başlattı. Anonymous işkencelerin devam etmesi durumunda oradaki görevlilerin tüm kişisel bilgilerini yayınlayacaklarını söyledi. Yetkililerin durumun ciddiyetini anlamaları için banka hesaplarına saldıran Anonymous ele geçirdiği 500.000$'ı da başta Kızılhaç olmak üzere hayır kurumlarına bağışladı (Kaliç, 2012:56-57). Bütün bu olayların sonunda Manning 2012 Nobel Barış Ödülüne aday gösterildi. Manning 'i ihbar eden Adrian Lamo ise 14 Mart 2018 tarihinde Wichita, Kansas'taki evinde ölü bulundu.

Wikileaks 'in kurucusu Jullian Paul ASSANGE hükümetlerin halktan bir şey saklama hakkının olmadığını bilginin evrensel olduğunu ve herkes tarafından erişilebilir olması gerektiğini savunmaktadır. 2010 Kasımında Wikileaks, ABD'nin gizli diplomatik belgelerini de yayımlamaya başlayınca, ABD iyice zor durumda kaldı. Yayımlanana belgelerde Türkiye' de dâhil olmak üzere birçok ülkenin yöneticileri hakkında akla gelebilecek her türlü bilgi belge ve fikir en gayrı resmi dille açıklanıyordu (Kaliç, 2012:53). Sonrasında açık ekonomiyi, liberalizmi, çok uluslu şirket yapısını, küreselleşmeyi savunan ulus devlet fikrine karşı çıkıp iş hayatında profesyonel davranılması gerektiğini savunan ABD'nin, dünyanın ödeme sistemlerini elinde tutmaya çalıştığı PayPal, Visa ve MasterCard gibi sözde profesyonel şirketleri, hiçbir sebep belirtmeden Wikileaks 'in bağış kampanyalarında toplanan paralara el koydular. Bu olay ve Güney Kıbırs-Yunanistan krizinde devletlerin banka mevduatlarında kesintiler yapması gibi Profesyonel hareketler Bitcoin gibi merkezi olmayan ödeme sistemlerinin desteklenmesinde önemli rol oynamıştır. Wikileaks 'e karşı yapılan bu hamle sonucunda Anonymous olarak bilinen hack gurubu Wikileaks 'i desteklediklerini duyurdu. Visa, MasterCard ve Paypal başta olmak üzere Wikileaks karşıtı tutum sergileyen finans kuruluşlarına "Assange'ın İntikam Operasyonu" kod adıyla siber saldırılar gerçekleştirdiler. Saldırılar sonucunda hem Visa hem de MasterCard'ın siteleri çökertildi (Kaliç, 2012:55). Bu olaylardan sonra da Wikileaks e yönelik saldırılar artarak devam etti. Veri güvenliği alanında faaliyet gösteren Kalifornia merkezli HBGary Federal firmasının 50.000 e yakın e-postasını ele geçiren Anonymous yazışmalar arasında Wikileaks'e yönelik karalama kampanyaları ve yasanın dışına çıkmak pahasına planlar yazılı bir dizi doküman tespit etti. Bu planlar arasında: başta Glenn Greenwald olmak üzere Wikileaks destekçisi gazetecilere yönelik karalama kampanyaları düzenlenmesi; Wikileaks 'e sahte belgeler sızdırılarak sonrasında bunların sahte olduklarını açıklanması

ve Wikileaks'in kaynaklarını açıkladığına yönelik söylentiler yayarak itibarsızlaştırılması hatta Wikileaks sisteminin siber saldırılar yaparak çökertilmesi gibi bir dizi hukuk dışı faaliyet yer almaktaydı (Ertem & Uçkan, 2011:110). Sonrasında ABD tarafından hakkında yakalama kararı çıkartılan Jullian Paul ASSANGE yurt dışında yaşamaya başlamıştır. Sürekli ülke değiştiren Assange 2006 yılında İsveç'te bir konuşma yapmak için bulunduğu esnada iki kadına tecavüz ettiği iddiası ile hakkında İsveç tarafından uluslararası yakalama kararı çıkarılmıştır. O esnada İngiltere'de bulunan Assange gözaltına alınmış ve kefaretle serbest bırakılmıştır. İngiltere'de ev hapsinde bulunduğu esnada 14 Haziran 2012'de İsveç'e iade edilmesi kesinleşince Londra'da ki Ekvator Büyükelçiliği'ne sığındı. 7 yıl Ekvator Büyükelçiliği'nde yaşayan Assange 11 Nisan 2019'da Londra polisi tarafından tutuklandı. Yargılaması hala devam etmektedir.

Devletler genelde istihbarat servislerinin masraflarını örtülü ödenek denilen miktarı bilinmeyen ödeneklerden karşılarlar. Bunun en önemli nedeni yaptıkları operasyonların büyüklüğü hakkında çalışan sayısı hakkında harcamalarından yola çıkarak bir takım tahminler yürütülmesin önlemektir. Gizliliğin bu denli önemli olduğu konularda Wikileaks'in yayınladığı belgelerin yol açtığı ekonomik zararı hesaplamak neredeyse imkânsızdır. En basit örneğiyle Wikileaks'in yayınladığı belgelerde yer alan ABD'nin diğer ülkelere karşı yürüttüğü gizli planlarını öğrenen, ülkeler ABD ile olan ilişkilerini tekrar gözden geçireceklerdir. Belki de milyon dolarlık yatırımların veya antlaşmaların başka ülkelerle yapılmasına neden olacaktır. Belgelerde açıklanan ABD'nin karşı operasyon yürüttüğü ülkelerle arasındaki ilişkileri tekrar eski haline getirmesi yıllarını alacaktır ve iyi niyet göstergesi olarak belki de milyonlarca dolara mal olacak tavizler verilecektir. Belgelerde açıklanan bir diğer husus olan ABD askerlerinin savaş suçları işlemesi de gene ABD'yi savaş tazminatı davalarıyla karşı karşıya bırakacaktır.

ABD'nin bir takım finansal kuruluşlarının Wikileaks'i susturmak için Wikileaks'e toplanan yardımlara el koyması, belki de görüp görebileceğimiz en büyük dışsallıklardan birini doğurarak bu şirketlerin güvenilmez olduğunu düşünün insanların akın akın bitcoin kullanımına geçmesine neden olmuştur. Ayrıca bu firmalar Wikileaks'e karşı olan tutumlarından dolayı Wikileaks'i destekleyen Anonymous'un hedefi haline gelerek gene milyonlarca dolar zarara uğramışlardır. Ve son olarak gene hükümetler Wikileaks sızıntılarından sonra veri güvenliklerini arttırmak için bir dizi ekstra önlem almışlar ve harcamalar yapmışlardır.

3.17 2007 ESTONYA VAKASI

Sovyetler birliği Nazi işgalinden kurtardığı tüm Doğu Avrupa ülkelerine dev bronz Rus askeri heykelleri dikmiştir. Rusya ikinci dünya savaşında Estonya'yı Nazi işgalinden kurtardıktan sonra buraya da bronz bir Rus askeri heykeli dikmiştir (Clarke & Knake, 2011:13,14). Estonyalıların çoğunluğunun, Sovyetler Birliğinin baskıcı 50 yılını hatırlatan bronz kızıl ordu askeri heykelini kaldırmak istemesi üzerine "Bronz Gecesi" denilen 26 Nisan 2007 tarihinde Estonya'da yaşayan etnik Ruslar ve Estonyalılar arasında yaşanan gerginlik büyümüştür (Kara, 2013:56). Devam eden süreçte gerginlik siber boyuta taştı ve bazı Rus sitelerinin siber saldırıların nasıl yapılacağını tarif etmesi olayları çığırından çıkardı ve Kâğıtsız Hükümet olarak anılan birçok devlet sisteminin internete adapte olduğu Estonya hükümeti işlemez hale geldi (Eren, 2017:59,60). Estonya'ya saldırı düzenleyen köle bilgisayarların kontrol merkezinin Rusya'da olduğu ve programın da Kiril alfabesi ile yazıldığı tespit edildi. Estonya konuyu NATO ya taşıyarak yardım istedi. Rusya saldırılarla bağlantısını reddetti fakat Estonya'nın saldırıların durdurulması ve saldırganların yakalanması yönündeki taleplerinin de reddetti (Çifci, 2017:184). Süreçle ilgili BBC nin yapmış olduğu haberin çevirisi aşağıdadır.

> *Estonya, ülkenin web sitelerinin son üç haftadır ağır saldırı altında olduğunu ve Rusya'nın siber savaşta yer almasından sorumlu tutulduğunu söyledi. Tallinn, saldırıların çoğunun Rusya'dan geldiğini ve Rus devlet bilgisayar sunucuları tarafından barındırıldığını söylüyor. Moskova ise iddiaları reddediyor.*
>
> *Estonya, saldırıların Tallinn'deki bir Sovyet savaş anıtı taşınmasından sonra başladığını söyledi. Hareket Kremlin tarafından kınandı. Bir Nato sözcüsü, örgütün Estonya'ya teknik yardımda bulunduğunu söyledi. NATO sözcüsü James Appathurai BBC News'e verdiği demeçte, "21. yüzyılda sadece tank ve toplarla ilgili değil. Estonyalı yetkililerin savunmaları konusunda kendilerine yardım etmeleri talebiyle uzmanlarımızdan birini gönderdik."*
>
> ***Kâğıtsız hükümet***
>
> *Estonya konuyu Cuma günkü AB-Rusya zirve gündeminin en üstüne koymak istiyor. Estonya savunma bakanlığındaki BT güvenliği başkanı Mikhail Tammet, BBC News'e yaptığı açıklamada, saldırıların parlamento ve devlet kurumları dâhil olmak üzere bir dizi internet sitesini etkilediğini söyledi. Ülkenin hükümeti çevrimiçi olarak yönetildiği için özellikle savunmasız olduğunu söyledi. "Estonya büyük ölçüde internete*

bağlı. E-devletimiz var, devlet kâğıtsız olarak adlandırılıyor. Tüm banka hizmetleri internette. Meclisimizi bile internet üzerinden seçiyoruz." dedi. Anıtın kaldırılması, Estonya'daki çoğu etnik Rus arasında bir kişinin öldüğü ve 150'den fazla kişinin yaralandığı isyanları da tetikledi. Estonyalılar, anıtın Baltık devletinin Sovyet işgalini sembolize ettiğini söylüyor. Ruslar bunun Nazilerle savaşanlara bir hediye olduğunu söylüyor.

Spam Seli

Estonya hükümeti, devlet ve ticari web sitelerinin, çok sayıda banka da dâhil olmak üzere sunucularının kitlesel DDOS ataklarıyla bombalandığını söylüyor.

Hizmet reddi saldırılarının hedefleri arasında Estonya dışişleri ve savunma bakanlıkları ile önde gelen gazete ve bankalar da yer aldı. Yetkililer saldırıya uğramamak için Estonya dışındaki sunuculara erişimi engelledi.

Estonyalı gazeteci Aet Suvari BBC'ye verdiği demeçte, 'Birkaç hafta önce her şey başladığında, çevrimiçi hizmetlerimizde bazı sorunlarımız oldu ve ardından posta sunucumuz da spam e-postalarla doldu,' dedi. 'Son birkaç haftada bazı devlet görevlilerinin e-postalarını internette okuması, bankalara ulaşması oldukça zor oldu.'

Savunma bakanlığı, siber saldırıların dünyanın her yerinden geldiğini ancak bazılarının Rus devlet sunucuları tarafından barındırıldığını söyledi. Siber savaşın nasıl yapılacağına dair talimatların Rusça web sitelerinde Rusça yayın yaptığını söylüyor. Estonya Başbakanı Andrus Ansip, doğrudan Rusya'yı sorumlu olmakla suçlayarak Rus hükümetini işaret etti. Nato ve AB internet uzmanları suçluların izini sürmekte yardımcı oluyorlar, ancak Estonyalı yetkililer Rusya ile işbirliği yapmadıklarını söylüyorlar.

Öncü Saldırı

Teknik uzmanlar ilk saldırı dalgasının Rusya'daki resmi yapılardan geldiğini söylese de, failleri takip etmenin çok zor olabileceğini söylüyorlar.

Uzmanlar Botnetlerin hizmet reddi saldırıları düzenleyen bilgisayar gruplarına verilen isim olduğunu birçok ülkede, hatta kıtalarda bulunabileceklerini belirtti. Büyük bir bilgisayar korsanları ve bilgisayar virüsü yazarları topluluğuna sahip olan Rusya, daha önce ABD ve Ukrayna'da bu tür saldırıları yapmakla suçlanıyor. Moskova, Estonya'ya yapılan internet saldırılarına katıldığını reddetti. Kremlin sözcüsü Dmitry Peskov BBC'ye iddiaların 'tamamen yanlış' olduğunu söyledi (http://news.bbc.co.uk/2/hi/europe/6665145.stm, 9.7.2019).

Bir heykelin kaldırılmasından çıkan bu kriz, siber ortama taştıktan sonra iki devlet arasında diplomatik bir krize dönüşmüştür. Sonrasında gelişen süreçte NATO'da olaya dâhil olmuştur. İlk dalga ekonomik etki olarak süreç boyunca Estonya hükümetinin yüksek teknolojik entegrasyonundan kaynaklı olarak hemen hemen hiçbir kamu hizmetini sağlayamaması sonucu ortaya çıkan ekonomik etki söz konusudur. Birçok siber güvenlik uzmanının dillendirdiği gibi bu tür teknolojiler iki ucu keskin bir bıçak gibidir. Teknoloji olmadan verimlilik tam olarak sağlanamamakta, fakat aynı zamanda yüksek teknolojik entegrasyon da Estonya örneğinde olduğu gibi beraberinde bir takım güvenlik risklerini de getirmektedir.

Bu örneğin neden olduğu en önemli dışsallıklardan biri ise Estonya hükümetinin yaşadığı siber güvenlik krizini NATO gündemine taşımasıyla birlikte NATO'nun siber güvenlik strateji eylem planları geliştirmesine neden olmasıdır. İzlenen bu yaklaşım sonucunda NATO üyesi birçok ülke siber güvenlik konusunda araştırma, geliştirme ve strateji eylem planları hazırlama için bir dizi harcama yapmışlardır. Bunlara ek olarak birçok ülke siber güvenlik komutanlıkları kurmuşlardır. Toplamı göz önüne aldığımızda Estonya örneğinin neden olduğu dışsal etki gene ilk çıkış etkisinden kat kat fazladır.

Ayrıca Estonya vakasını gözlemleyen diğer devletlerde bu olayın yansımaları muhtemel iki tür tepkiye neden olacaktır. Ya teknolojik entegrasyonun güvensiz olduğunu düşünerek teknoloji yatırımlarını ağırdan alacaklardır ve bu durumda teknoloji firmalarına gelir kaybı olarak yansıyacaktır. Yada teknoloji yatırımı yaparken siber güvenlik konusuna da ağırlık vereceklerdir ve bu durumda da siber güvenlik firmalarında gelir artışına neden olacaktır. Bu olayın neden olabileceği bir diğer dışsallık ise Estonya'da yaşayan Sovyet kökenli vatandaşlar ile Estonya halkı arasında belki de hiç onarılmayacak derin yaralar açmış olmasıdır. Bu olayda problem derinleşmemiştir fakat Arap Baharı olaylarında gözlemlendiği üzere bu tür toplumsal ayrışmaların sonu iç savaşa kadar gidebilmektedir. Günümüze gelindiğinde ise bu olaydan ders alan Estonya siber güvenlik konusunda ciddi yatırımlar yapmıştır. Sonuç olarak Rusya'nın Estonya'ya karşı başlatmış olduğu siber saldırıların ekonomik dışsallık etkileri, saldırıların Estonya hükümetinde yol açtığı ilk dalga etkiden çok daha fazla ekonomik etkiye neden olmuştur. Ayrıca Rusya'nın el altından saldırganlara teknik destek vermesi ve desteklediğini reddetmesi de bu olayı, siber alana taşınmış vekâlet savaşlarına iyi bir örnek haline getirmektedir.

3.18 2007 İMKB FİBER OPTİK KABLO VAKASI


255 milyar dolarlık borsaya kepçe darbesi

refid:7777722 ilişkili resim dosyası

Kavşak inşaatı çalışmaları sırasında bir kepçe operatörünün fiber optik kabloyu koparması yüzünden dün İMKB'de işlemler ancak 14.30'da başlayabildi ve tek seans yapılabildi. Geniş bir kitleyi etkileyen arıza ile ilgili olarak inşaat şirketi hakkında tazminat davası açılacak. İMKB yönetiminin bugünkü genel kurulda arıza ile uğranan kaybın tazmin edilmesini görüşmesi bekleniyor.

Şekil 21: İstanbul Menkul Kıymetler Borsası Fiber Optik Kablo Vakası

Kaynak: Hürriyet

28 Kasım 2007 tarihinde kavşak inşaatı çalışması esnasında bir kepçe operatörünün yanlışlıkla fiber optik kabloyu koparması nedeniyle ertesi gün saat 14.30'a kadar İMKB'de işlemler yapılamamış, büyük maddi zarar meydana gelmiştir

(http://www.hurriyet.com.tr/gundem/255-milyar-dolarlik-borsaya-kepce-darbesi-7777722 9.7.2019) (Kara, 2013:48).

Bu olay bir siber saldırı mıdır değil midir tartışılır. Kepçe operatörünün niyetini bilemeyiz. Fakat bir siber saldırı olduğunu varsayarsak ilk etki olarak borsanın kapandığı süre boyunca borsanın işlem hacminin büyüklüğü kadar bir ekonomik etkisi olacaktır. Bu sürenin neredeyse bir gün olduğunu göz önünde bulundurursak zarar oldukça büyüktür. Fakat dışsallıklar açısından gene alınacak bir takım ekstra güvenlik önlemleri yatırımlar ve borsanın imajının sarsılması gibi bir takım dışsal etkilere neden olacaktır. Bu olayın sonucunda borsanın puanı düşecektir ve bu da ekstra bir maliyet demektir.

3.19 2008 RUSYA – GÜRCİSTAN VAKASI

2003 yılında Gürcistan'ın Güney Osetya'ya saldırması ile birlikte Rus Hackerlar Gürcistan devlet sitelerine saldırılarak internet sitelerine propaganda görüntüleri yerleştirildi ve Gürcistan'ın internet alt yapısını çökertti. Ruslar www.stopgeorgia.com sitesini kurarak herkesi gönüllü saldırı yapmaya davet ettiler. Gürcistan devlet siteleri ile birlikte ABD ve İngiltere sitelerini de çökerttiler. 21 Temmuz 2008'de yapılan saldırlar sonucunda Gürcistan Dış İşleri Bakanlığı'nın internet sitesinin erişime kapatılması sonucunda Gürcistan Rusya merkezli IP adreslerini engelledi. Bunun üzerine Ruslar saldırılarına Estonya, Kanada, Türkiye ve Çin'deki köle bilgisayarlar üzerinden devam ettiler (Çifci, 2017:186). Bu örnekte siber saldırıların diğer ülkelere karşı bir baskı aracı olarak nasıl kullanılabildiğini görmekteyiz. Tıpkı ABD'nin Irak'ta yaptığı gibi Rusya'da hedefine koyduğu Gürcistan'ı psikolojik olarak yıpratmaya çalışmaktadır. Bu tür saldırılarda amaç genelde savaş öncesi ortamı hazırlamaktır. Nitekim Rusya Gürcistan'ın bazı bölgelerini işgal etmiş durumdadır. Ve saldırıları boyunca ne tür istihbarat bilgileri elde ettikleri bilinmemektedir. Bu tür saldırıların ekonomik boyutu sadece sistemlerin işlemez hale gelmesi değildir. Çalınan bilgilerin değerine ve kullanım alanlarına göre değişebilmektedir.

3.20 2009 İSTANBUL ATATÜRK HAVALİMANI VAKASI

Şekil22: İstanbul Atatürk Havaalanına Siber Saldırı

Kaynak: CNNTürk

Atatürk Havalimanı'nın işletici firması TAV tarafından yapılan açıklamada, Türkçe karşılığı "Ağa karışmış solucan" olarak tanımlanan "Downadup" adlı virüsün, bugün erken saatlerde Dış Hatlar Terminali'ndeki işlemlerde sorun yarattığı, bunun üzerine bilet ve bagaj işlemlerinin elle yapıldığı bildirildi. Açıklamada, virüs nedeniyle 400'e yakın sistem merkezinde virüs temizlemesi yapıldığı ve işlemin devam ettiği ifade edilerek, "Bu problem nedeniyle SITA yetkililerinden alınan bilgiye göre SITA sistemlerinin kullanıldığı Los Angeles, Miami, Oslo, JFK, Orlando ve Bremen gibi önemli hava limanlarında sorun yaşanmıştır" denildi

(https://www.cnnturk.com/2009/bilim.teknoloji/teknoloji/01/30/bilgisayar.virusu.ataturk.havalimanini.felc.etti/511371.0/index.html) 9.7.2019).

Saldırıda ilk dalga ekonomik etki olarak aksayan yolcu işlemleri sonucu geç kalkan veya kalkamayan uçaklar olarak görülmektedir. Fakat dışsallıkları göz önüne aldığımızda bu olay sonucu bir ihaleye geç kalan bir iş adamının kaybı da bu siber saldırının sonucudur. Bir diğer dışsallık etkisi veya ardıl etkisi de aktarmalı uçuşlarla

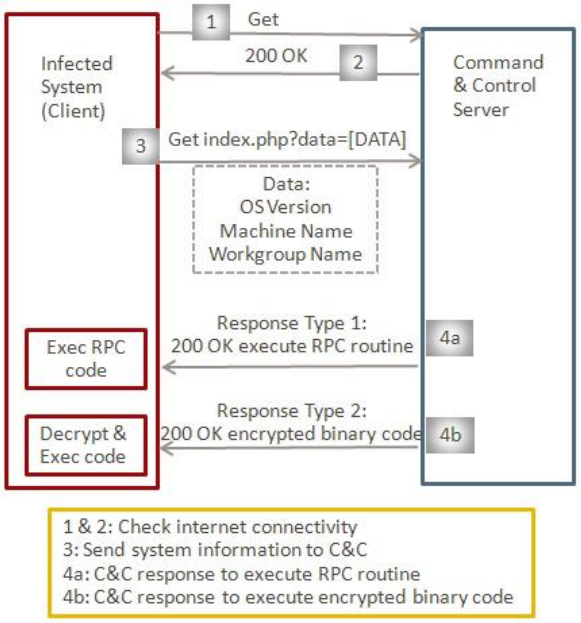
farklı noktalara gidecek olan yolcuların İstanbul havaalanından kalkamadıkları için aktarma noktalarına zamanında varamamaları sonucunda uçaklarını kaçıracak olmalarıdır. Havayolu firmaları bu zararı tazmin eder mi bilinmez fakat tazmin ederlerse bile bu sefer havayolu firmalarının yaptıkları bu telafi harcamaları da gerçekleşen siber saldırının maliyet hanesine eklenmelidir. Ardıl etkiler veya dışsallıklar burada da sona ermiş değildir. Uçakları siber saldırı nedeniyle geç kalkan dolayısıyla aktarma noktasına zamanında yetişemediği için bir sonraki uçuşu bekleyen yolcular normalde gidecekleri yerde yapacakları harcamaları aktarma noktasında yapacaklardır. Bu harcamalar bir sonraki uçuşun ne kadar süre sonra olduğuna bağlı olarak değişecektir. Bu anlattıklarımız gibi daha pek çok ardıl etkisi, dışsallık mevcuttur. Burada en önemli nokta örnekte bahsi geçen siber saldırının maliyetinin sadece yolcuların bilet paraları olmadığının anlaşılmasıdır. İş antlaşması, ihale veya bu tür yüksek düzeyde ticari ilişkiler kurmak amacıyla seyahat eden iş adamlarının zararının bile uçak biletlerinin tutarından fazla olduğunu düşünebilirsiniz.

3.21 2010 STUXNET VE DUQU VAKASI

Beyaz Rusya'daki küçük bir firma olan VirusBlokAda tarafından, 2010 Haziranı'nda tespit edilen Stuxnet virüsü özellikle SCADA sistemlerine saldırmak üzere yazılmış, bilinen ilk ve en karmaşık yazılımdır. İncelemeler sonucunda Stuxnet'in basit bir solucan olmadığı karışık bir yapısı olduğu tespit edilmiştir (Kara, 2013:33).

Uranyum-235'in zenginleştirilmesi oldukça hassas bir denge gerektiriyor. IR-1 santrifüjleri dakikada 100.000 rotasyona ayarlıydı. Daha yavaş döndüğünde nükleer enerji elde edilemiyor daha hızlı döndüğünde ise IR-1 santrifüj makineleri yanıyor ve devreden çıkıyordu. Stuxnet devreye girdiğinde önce kendini kopyalayarak diğer makinelere 'de bulaşıyor, daha sonra binlerce santrifüjü etkileyerek delirtiyor durup dururken bir yavaş bir hızlı dönmelerine neden oluyordu. Ve bütün bunlar olurken Stuxnet SCADA sistemlerinin normal çalıştığının görünmesini de sağlıyordu. Stuxnet virüsü İran'ın Natanz Uranyum Zenginleştirme Merkezi'nin çalışmalarını uzunca bir süre sekteye uğratmıştır. Natanz'ın entegre makine ekipmanları Siemens tarafından kurulmuştu. Santrifüjler Siemens'in S7-417modeliydi, kontrol ünitesi de gene Siemens uygulamasıydı (Eczacıbaşı, 2018:178).

Stuxnet'in algoritması aşağıdaki gibidir.



Şekil 23: Stuxnet Algoritması
Kaynak: Symantec Stuxnet Raporu

Symantec siber güvenlik şirketinin 2010 Stuxnet Raporu'nun çevirisinde Stuxnet Virüsünün işleyişi anlatılmaktadır:

Stuxnet kendini kurduktan sonra, İnternet erişiminin tehlike altındaki bilgisayardan mümkün olup olmadığını belirlemek için www.mypremierfutbol.com www.todaysfutbol.com sunucuları ile bağlantı kurmaya çalışır. Bağlantı kurulduktan sonra C&C (Command And Control – Komuta Kontrol) sunucularından dosyalarını indiriyor ve sistemle ilgili

- *Windows sürüm bilgisi*
- *Bilgisayar adı*
- *Ağ grubu adı*
- *SCADA yazılımının yüklü olup olmadığına yönelik bilgiler*
- *Tüm ağ arabirimlerinin IP adresleri*

Bilgilerini topladıktan sonra topladığı verileri 31 baytlık bir anahtar kullanılarak XOR(Veri güvenliğinde blok şifreleme ailesine dâhil simetrik şifreleme temel şifreleme yöntemlerinden biri) ile şifreleyip 80 numaralı Port (bağlantı noktasındaki) C&C sunucusuyla bağlantı kurup bilgileri saldırgana gönderiyor. C&C sunucusundan

gelen cevaplarda gene farklı bir 31 bayt anahtar kullanılarak XOR ile şifrelenmiş olarak geliyor. Bu anahtarların her ikisi de, tehlike altındaki bilgisayardaki kötü amaçlı. dll dosyasında bulunur ve C&C sunucusuna gelen ve giden ağ trafiğini deşifre etmek için kullanılabilir.

Ayrıca Stuxnet kendini yeni C&C URL'leri ile güncelleme kabiliyetine sahiptir ancak henüz güncellenmiş konfigürasyonlara sahip herhangi bir dosya tespit edilmemiştir.

C&C bu bilgiyi aldığında 2 tip cevap ile cevap verebilir. İlk müdahale türü, tehdide tehdit kodu içerisinde zaten mevcut olan prosedürlerden birini yerine getirme talimatını verir. Aslında, bu yanıt türündeki veriler, ana. dll dosyası içindeki çeşitli RPC(Remote Procedure Call- Uzak yordam çağrısı) yordamlarına iletilir. İkinci yanıt türü, istemciye yanıtta ek bir. dll dosyası sunar ve istemciden bu. dll dosyasını yüklemesini ve sıradan bir çağrı yapmasını ister.

İlk yanıt türü, yerel makineye iletilecek olan RPC'ler için bir kabuk görevi görür. İstemci tarafında gerçekleştirilen RPC çağrıları aşağıdaki işlemleri gerçekleştirebilir:

- *Bir dosyayı okuma*
- *Bir dosyaya yazma*
- *Bir dosyayı silme*
- *İşlem oluşturma*
- *lsass.exe içine bir .dll enjekte etme*
- *Ek bir .dll dosyası yükleyerek çıkış 1 i çalıştırma*
- *Ana kaynak dosyasından kaynak 210'u çıkarın (bu kaynak diğer işlemlere enjekte etmek için kullanılır)*
- *Tehdit için yapılandırma verilerini güncelle*

(https://www.symantec.com/connect/blogs/w32stuxnet-network-operations, 09.07.2019).

Stuxnet virüsü üreticilerinden biri Finlandiya'da diğeri ise İran'da olan 807 herz ile 1200 hertz arasında çalışan frekans çeviricilere sahip SCADA(Supervisory Control And Data Acquisition- Endüstride sıkça kullanılan Denetleme Kontrol ve Veri Toplama sistemleri) arayıp bulduğunda çıkış frekanslarını arttırarak hedef sistemin bozulmasına yol açacak şekilde tasarlanmıştır. Ayrıca Alman bilgisayar uzmanı Ralph Langner ve ekibinin araştırmalarına göre Stuxnet bünyesinde en az dört yeni zero-day(0-day, sıfırıncı gün) açığı bulundurmaktaydı. Hackerlar 0-day açıklarına değer verir ve mecbur

kalmadıkça açıklamaz veya kullanmazdı. Mevcut bir açık kapı varken dördünü tek seferde kullanılması bir ilkti ve dikkat çekiciydi. Bunlara ek olarak Stuxnet iki ayrı ünlü şirketten çalınmış dijital imzalı sertifika anahtarları ile 10 yaşındaki Windows 95 sürümüne kadar tüm Windows işletim sistemlerinde çalışabilecek hale getirilmişti (Singer & Friedman, 2015:158). Bu tür saldırıları yapmak yılların planlamasını gerektirir ve milyonlarca dolara mal olabilir. Neyse ki kendi siber silahlarını üretecek kadar zamanı ve bütçesi olmayanlar için Darknet'te sıfır gün açıkları satılan karaborsalar bulunmakta (Goodman, 2016:309).

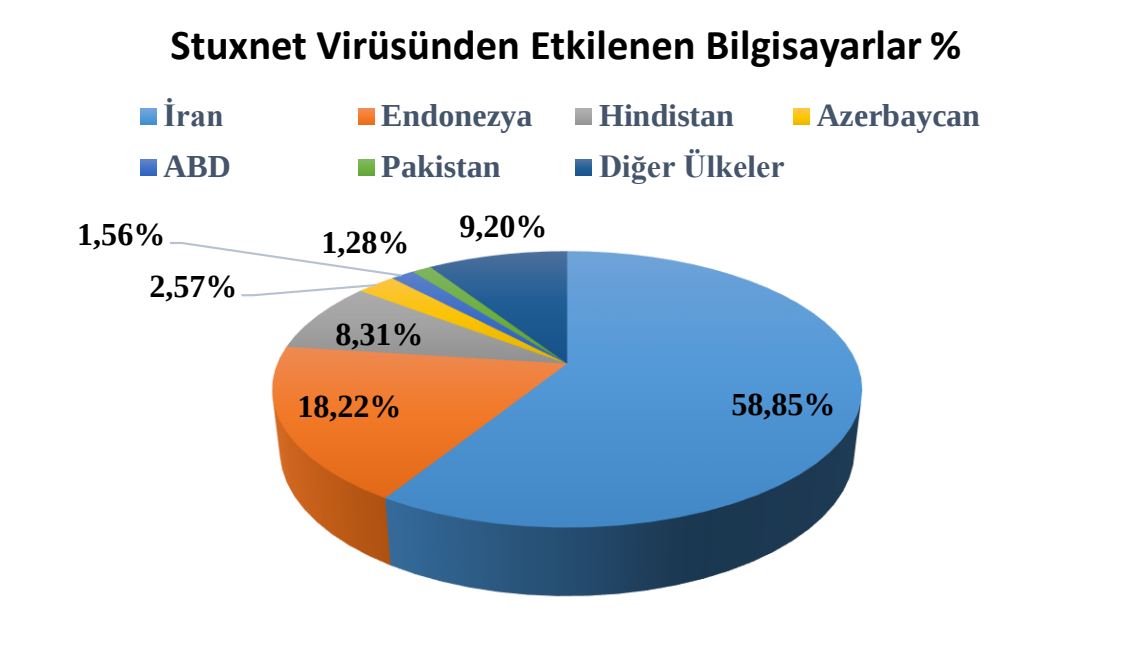
Bütün bunlardan anlaşıldığı üzere Stuxnet 'i internete salanlar oldukça geniş kaynaklara sahip ve hedefi iyi tanıyan, işi garantiye alan, hedefin mutlaka yok edilmesini isteyen kişilerdir. Bu denli bir motivasyon ve imkan ancak devletlerde bulunabilir. Çoğu uzmanın yorumu da bu virüsün arkasında bir devletin olduğu yönündedir. ABD veya İsrail'den şüphelenilmektedir fakat henüz resmi bir açıklama gelmemiştir.

Stuxnet virüsünden etkilenen bilgisayarlar yüzdelik olarak aşağıdaki tabloda verilmiştir.

Tablo 7: Stuxnet'ten Etkilenen Ülkeler

ÜLKE	Etkilenen Bilgisayar %
İran	%58,85
Endonezya	%18,22
Hindistan	%8,31
Azerbaycan	%2,57
ABD	%1,56
Pakistan	%1,28
Diğer Ülkeler	%9,2

Kaynak: Çifci, 2017:191



Grafik 24: Stuxnet Virüsünden Etkilenen Bilgisayarların % Dağılımı

Kaynak: Tablo 7'teki veriler Kullanılarak Tarafımızdan Oluşturulmuştur

Stuxnet vakası siber güvenliğe yönelik algıları kökünden değiştirmiştir. Siber saldırıların bir savaş aracı olarak veya siyasi bir araç olarak kullanılmasının en önemli ve öncü örneklerindendir. Çoğu uzman bu tür bir saldırıyla bir nükleer tesisin sabote edilip nükleer bir felakete yol açabileceği konusunda hem fikirdir. Stuxnet vakasının Natanz nükleer tesisi çalışanlarından birinin kişisel usb belleğini tesisteki bir bilgisayarda kullanması ile başlamış olabileceği düşünülmektedir.

Tablo 8: Stuxnet Sonrası Değişen Algı

Önceki Kabuller	**Stuxnet Sonrası Öğrenilenler**
Kontrol sistemleri dış ağlardan izole edildiğinde siber saldırı riski ortadan kalkar.	Kontrol sistemleri halen insan unsuruna bağımlıdır: güçlü bir güvenlik; dikkatsiz/ meraklı bir kullanıcı, taşınabilir aygıt veya zayıf farkındalık ile aşılabilir.
Modern sayılabilecek sistemleri yönetmeyen PLC ve RTU lara saldırı ihtimali yoktur.	PLC'ler hedef alınabilir ve zararlı yazılımlardan etkilenebilirler.
IDS/IPS ve Güvenlik duvarları kontrol sistemlerini saldırılardan korumak için yeterlidir.	İmza ve kod tabanlı tespit ve önleme sistemleri yeterli değildir. Bilinmeyen saldırıların tespitine yönelik geniş kapsamlı savunma sistemlerine odaklanılmalıdır.
SCADA ve benzeri sistemlere erişmek kolay değildir. Etkili bir saldırının gerçekleşmesi imkânsızdır.	Motivasyon, niyet ve yeterli kaynak var olduğu sürece saldırılar mümkündür.

Kaynak: Meral, 2015:75

Duqu Virüsü

Duqu virüsü ise Stuxnet' ten yaklaşık bir yıl sonra 1 Eylül 2011'de tespit edilmiştir. Yapısal açıdan Stuxnet'le birçok benzer yönü bulunmakla beraber zarar vermek için değil endüstriyel sistemler hakkında detaylı bilgi toplayarak benzerlerini oluşturmak veya Stuxnet gibi saldırılara öncü keşif gücü olarak hizmet vermek amacıyla yapıldığı düşünülmektedir (Aytekin, 2015:22).

3.22 2012 155 POLİS İHBAR HATTI VAKASI

Ankara Emniyet Müdürlüğü'nün sistemine giren internet korsanları polise gönderilen ihbarları ele geçirdi.

Şekil 24: RedHack
Kaynak: https://www.ntv.com.tr/turkiye/kizil-hackerlar-polis-sistemini-hackledi,3w7o4PZrQUaj55JEzb2NRA

Ankara Emniyet Müdürlüğü'nün bilgisayar sistemini hackleyen internet korsanları, güvenlik şubesine yönlendirilen bazı belgeleri ele geçirmeyi başardı.

Kendilerine 'Kızıl Hackerlar' adını veren korsanlar, şifresini kırarak girdikleri Ankara Emniyet Müdürlüğü bilgisayar sisteminden çaldıkları belgeleri internet sitelerinden "Polisin Gizli Belgelerini ve Muhbirlerini Açıklıyoruz!" başlığıyla yayınladı (https://www.ntv.com.tr/turkiye/kizil-hackerlar-polis-sistemini-hackledi,3w7o4PZrQUaj55JEzb2NRA, 1.7.2019*).*

RedHack grubundan birisinin hackledikleri polis merkezinin şifresinin 123456 olduğunu söyleyip durumla dalga geçmesi üzerine sorumlu bulunan iki polis ve sivil memura maaş kesme cezası verildi. Devam eden süreçte 27 Mart 2012 Tarihli Emniyet

Genel Müdürlüğü Genelgesi ile personele ve kuruma ait tüm hesaplar için şifre oluşturma standardı yayımlandı (Gökdemir, 2013:69-71).

3.23 2013 ASSOCİATED PRESS HABER AJANSININ HACKLENMESİ

ABD'de oldukça tirajlı bir haber ajansı olan Associated Press haber ajansının Twitter hesabı 23 Nisan 2013'te kendilerine Suriye Electronic Army (SEA) diyen bir grup Suriyeli hacker tarafından hacklenmiştir. Ele geçirilen Twitter hesabından SEA'nın "Beyaz Saray'da iki patlama oldu, Obama yaralandı." Şeklinde asılsız haberler paylaşması, Dow Jones endeksinde 140 puanlık bir düşüşe neden olmuştur (https://www.bbc.com/news/world-middle-east-22287326 1.07.2019).

Görünürde ilk olarak bir ekonomik etki yoktur fakat bu saldırı sonucunda ortaya çıkan dışsallıkların etkisi borsa ya yansımıştır. Bir bakış açısı kazandırması açısından iyi bir örnektir.

3.24 2014 EC-COUNCİL'İN HACKLENMESİ

Eugene Belford takma isimli bir hacker tarafından 23 Şubat 2014 tarihinde Amerika merkezli profesyonel etik hacker sertifikalandırma kurumu olan E-Commerce Consultants (EC-Coincil) hacklendi. Konsüle kayıtlı olan 60.000'den fazla etik hackerın kayıt esnasında kurum tarafından e-posta yoluyla talep edilen kimlik bilgileri yayınlandı. Kimlik bilgileri yayınlanan bilişim uzmanları arasında Amerikan Ordusu, FBI, Birleşmiş Milletler ve NSA çalışanları da var. Kurumu hackleyen hacker, ele geçirdiği kimlik bilgilerini hackerların hackledikleri siteleri kaydettikleri zone-h sitesinde "*Sertifikalı etik olmayan yazılım güvenliği uzmanına aittir.*" başlığıyla yayınladı (https://h4cktimes.com/siber-saldirilar-suclar/etik-hacker-kurulusu-ec-council-hacklendi-edward-snowdenin-pasaportu-yayinlandi.html, 5.1.2019).

Görünürde bu saldırıda da bir ekonomik etki yok gibidir. Fakat bu tür saldırılarda açıklanan verilerin nasıl kullanılacağına bağlı olarak ekonomik etkiler değişmektedir. Saldırıyı gerçekleştiren hackerın elde ettiği kimlik bilgilerini yayınlaması bu çalışanları hedef haline getirecektir. Ve bunun sonucunda da onların malına ve canına yapılan her saldırı bu siber saldırının ekonomik sonuçları toplumsal sonuçları olacaktır.

3.25 2014 ABD SERMAYE PİYASASINA SALDIRI

2014 yılında gerçekleştirilen ve en büyük boyutlu borsa sahteciliklerinden biri olarak kabul edilen soygunun davasına başlandı. Vadym Iermolovych adında Ukraynalı bir hacker, üç ekonomi e-dergisini ve kamu dışı finans bilgilerini ele geçirmekle ve bunları ticari faaliyetlerde kullanmakla suçlanıyor. Hackerlar kamuya açıklanmamış finansal bilgileri borsa oyuncularına satarak piyasaların manipüle edilmesine olanak tanımış, yayımlanmamış basın bültenlerinin yardımıyla elde edilen bu bilgilerle 30 milyon dolarlık soygun gerçekleştirilmişti.

ABD Adalet Bakanlığı, 28 yaşındaki Iermolovych'in, federal yargıcın elektronik sahtekârlık, hackerlık ve kimlik hırsızlığı suçlaması üzerine kimliğini ifşa etti. Yetkililer, hackerın 2014 yılında en büyük menkul kıymetler dolandırıcılığı olarak kayda geçen bilgisayar korsanlığından tutuklandığını ifade etti.

Soruşturmacılara göre Iermolovych; Marketwired, PR Newswire ve Business Wire'ın ağlarını ele geçiren şebekenin üyesi. Grup ise 150 binden fazla güvenilir finansal haberleri daha basılmadan basın bültenlerinden çalıp; bunları içerden bilgiyle menkul değer alıp satan ticaret adamlarıyla iş yapmaktaydı.

Federal savcı tarafından suçlanan üç hacker ve yedi borsacıdan oluşan grubun yanında, 40'tan fazla kişi de ABD Sermaye Piyasası Kurumu tarafından üstü örtülü uyarıldı.

Yetkililer; birçoğu Rusya ile bağlantılı olan borsacıların hackerlara, finansal rakamlarının artmasını istediği bir 'alışveriş listesi' verdiği ve sonra da pek çok şirketle ticari faaliyetler yürüttüğünü söyledi.

Şubat 2010'dan Ağustos 2015'e kadar devam eden dolandırıcılık faaliyetinin, oltalama saldırılarını içeren siber atak serisiyle başlayıp kar marjları ve kazançlarla ilgili bilgileri ele geçirmeleriyle devam ettiği bildirildi(https://siberbulten.com/siber-guvenlik/basin-bulteniyle-borsa-vurguncusu-hacker-hakim-karsisinda/ , 20.06.2019).

Bu örnekte NSA ve ECHELON gibi küresel dinleme sistemlerinin yaptıkları dinlemeleri nasıl paraya dönüştürdükleri hakkında bir fikir edinme açısından önemlidir. Buradaki fark bu sefer saldırıyı hackerlar yapmıştır ve elde ettikleri verilerle borsa da bir limon piyasa oluşmasına neden olmuşlardır. Ayrıca burada sözü geçen 30 milyon $ sadece hackerların cebine giren paradır. Saldırının neden olduğu ekonomik etki elbette kat kat fazladır.

3.26 ABD FEDERAL DEVLET KURUMLARININ PERSONELİNE YÖNELİK SİBER SALDIRI

ABD yönetimine bağlı Personel Yönetim İdaresi (OPM), nisan ayında siber saldırıya uğramıştı. OPM, tüm federal kurumlardaki personeli güvenlik taramasından geçiriyor. Personelin yetkilerinin belirlenmesinde kurumun önerileri esas alınıyor. Siber saldırıyı araştıran OPM yetkilileri, saldırıdan 21 milyon 500 bin dolayında vatandaşın etkilendiğini açıkladı. Bilgisayar korsanlarının federal kurumlarda halen görev yapan personelin yanı sıra eski çalışanların da kişisel verilerini ele geçirdiği açıklandı. Federal kurumlarda çalışmak üzere başvuruda bulunan milyonlarca kişinin kayıtları da hackerların eline geçti. Ayrıca hükümet kurumlarına dışarıdan hizmet veren şirketlerin yetkilileri ve yakın çevrelerine ait bilgiler bilgisayar korsanlarınca elde edildi.

İkamet adresi, sosyal güvenlik kimlik numarası, doğum, telefon, sağlık kayıtları, mali duruma ilişkin bilgiler ve sabıka kaydı, ele geçirilen kişisel bilgiler arasında yer alıyor. Veriler arasında bazı vatandaşların parmak izi de bulunuyor. ABD Federal Polis Teşkilatı (FBI) Başkanı James Comey saldırıyı "çok büyük bir sorun" olarak nitelendirdi. Comey, kayıtlarda personelin komşuları, arkadaşları ve akrabaları hakkında bilgiler, hatta ABD dışına yapılan geziler ve geziler esnasında temas kurulan kişiler hakkında da notlar yer aldığını söyledi. Siber saldırıdan Çin sorumlu tutulmuş, Pekin suçlamaların temelden yoksun olduğunu savunmuştu. Komşular ve akrabalar da korsanların 'elinde' İkamet adresi, sosyal güvenlik kimlik numarası, doğum, telefon, sağlık kayıtları, mali duruma ilişkin bilgiler ve sabıka kaydı, ele geçirilen kişisel bilgiler arasında yer alıyor. Veriler arasında bazı vatandaşların parmak izi de bulunuyor.

ABD Federal Polis Teşkilatı (FBI) Başkanı James Comey saldırıyı "çok büyük bir sorun" olarak nitelendirdi. Comey, kayıtlarda personelin komşuları, arkadaşları ve akrabaları hakkında bilgiler, hatta ABD dışına yapılan geziler ve geziler esnasında temas kurulan kişiler hakkında da notlar yer aldığını söyledi. Siber saldırıdan Çin sorumlu tutulmuş, Pekin suçlamaların temelden yoksun olduğunu savunmuştu(https://www.dw.com/tr/abdye-siber-saldırı/a-18574588 , 20.06.2019).

3.27 2014 ALMAN ÇELİK FABRİKASINA SALDIRI

Şekil 25: Alman Çelik Fabrikasına Saldırı
Kaynak: Teknopat, https://www.technopat.net/2014/12/23/hackerlar-almanyada-celik-fabrikasini-hackledi/ , 23.12.2014).

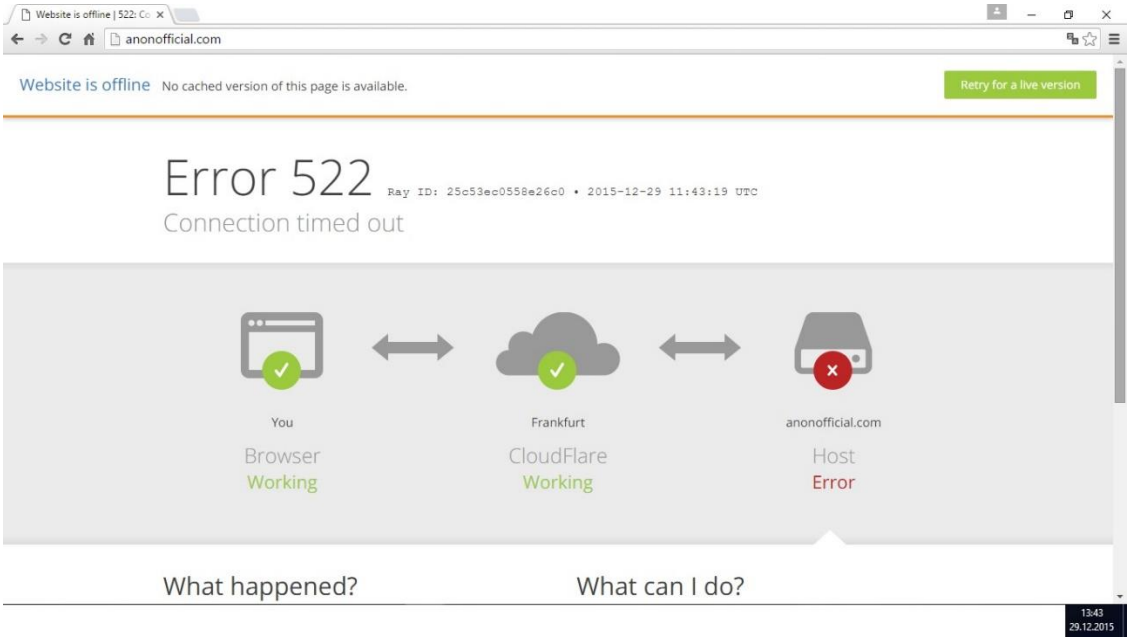
Almanya Resmi Bilgi Güvenliği Ofisi (BSI) tarafından yapılan açıklamaya göre saldırganlar bir çelik fabrikasını hackleyerek fiziksel zarara neden oldular. Karmaşık sosyal mühendislik ve spear phishing tekniklerini kullanan hackerlar, fabrikanın ofis ağına erişti. Spear phishing, saldırganların sanki bir organizasyondan geliyormuş gibi e-postalar gönderdiği bir saldırı tipi. Bu tür e-postalar ile ofis ağına erişen saldırganlar, buradan da üretim ağına sızdı. Bu aşamadan sonra ise bazı bileşenler ve hatta bütün sistemler çökmeye başladı. Fabrikanın maden eritme ocaklarından biri kontrollü bir biçimde kapatılamadı ve BSI'a göre bu durum fabrikada devasa zararlara yol açtı. Saldırganların teknik yeteneklerinden ise "çok gelişmiş" olarak bahsedildi (https://www.technopat.net/2014/12/23/hackerlar-almanyada-celik-fabrikasini-hackledi/ , 23.12.2014).

Bu saldırının dışsal etkisi de fabrika ile iş yapan tedarikçi firmalara ve fabrikanın tedarikçisi olduğu firmalara olacaktır.

3.28 2015 TÜRKİYE-RUSYA SİBER SAVAŞI

24.11.2015 tarihinde SU-24 tipi Rus uçağı Türkmen Dağı mevkiini bombalamak için sorti yaptığı esnada, hava sahamızı ihlal ettiği gerekçesiyle defaten uyarılmıştır. Uyarılara yanıt vermeyen Rus Uçağı Türk Hava Kuvvetleri tarafından düşürülmüştür. Bu olaydan sonra ülkemize karşı gerçekleşen siber saldırılar yoğunlaşmıştır. Anonymous denilen hacker grubu tarafından Türkiye'ye savaş açılmıştır. 14.12.2015 Tarihinde Anonymous'un DDOS saldırılarını yoğunlaştırması nedeniyle Türkiye'nin DNS sunucularını barındıran ODTÜ yetkilileri saldırılara karşı önlemler almıştır. Üç gün boyunca süren saldırılardan kaynaklı olarak internet erişiminde ufak çaplı yavaşlamalar olmuştur. ODTÜ yetkilileri saldırının büyüklüğünün tarihe geçecek boyutta olduğunu açıklamışlardır. Sonrasında gelişen süreçte Türk hacker grupları Ay Yıldız Team(AYT), Cyber Warrior Team (CW) ve Türk Hack Team (THT) başta olmak üzere Rusya'ya savaş açarak karşı atağa geçmişlerdir.

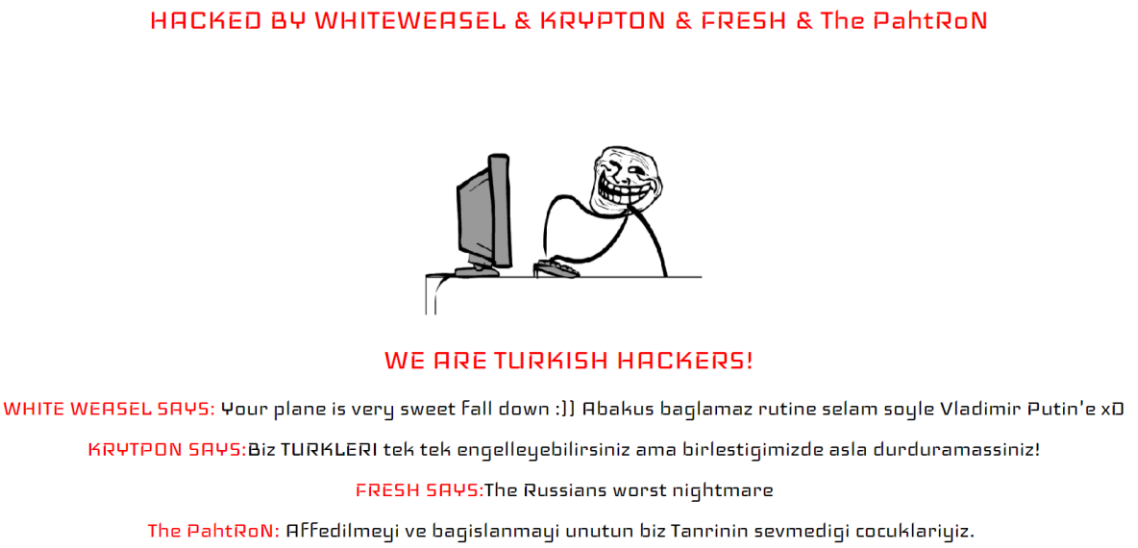
Anonymous 'a saldıran CW Anonymous sistemlerini erişime kapatmıştır.



Şekil 26: Anonoffical Sitesi Servis Dışı
Kaynak: Tarafımızdan ekran görüntüsü alınmıştır.

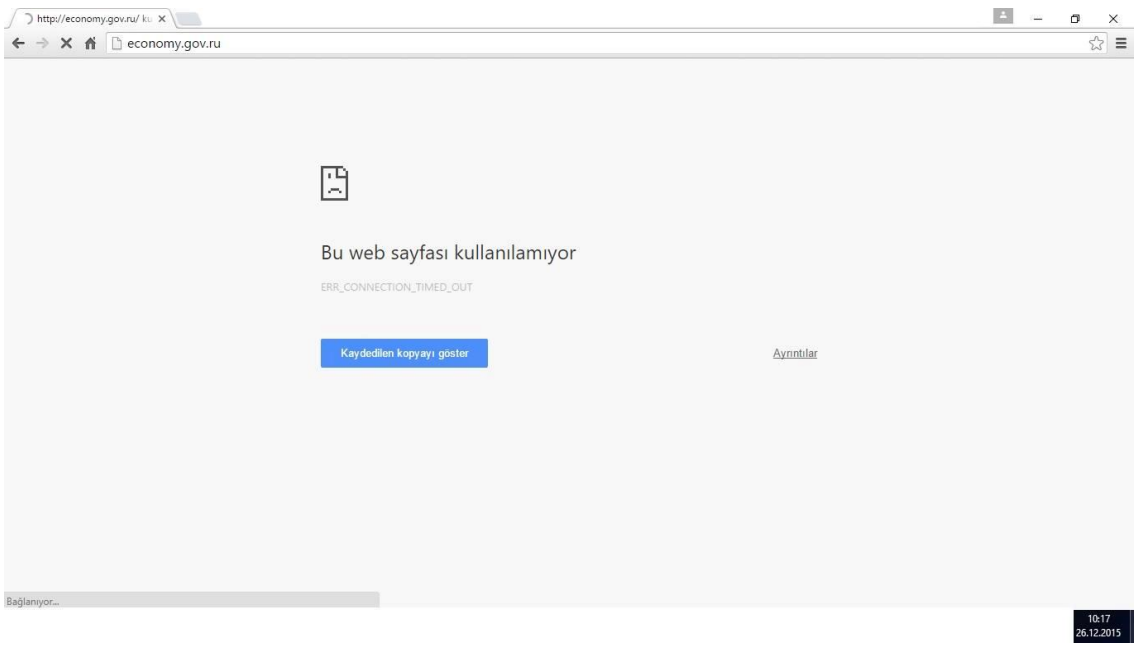
Türkiye cephesinde adeta seferberliğe dönüşen bu karşı ataklar sonucunda birçok Türk hacker timi olaya müdahil olmuştur.

Kimliği ve grubu bilinmeyen hackerlarca Rusya Ekonomi Bakanlığı'nın resmi internet sitesi hacklenmiştir.



Şekil 27: Rusya Ekonomi Bakanlığı'nı Hackleyen Hackerların Bakanlığın Sayfasına Koydukları Görsel
Kaynak: Tarafımızdan ekran görüntüsü alınmıştır.

Saldırılarla başa çıkamayan yetkililer bakanlığın resmi internet sitesini erişime kapatmak zorunda kalmışlardır.



Şekil 28: Rusya Ekonomi Bakanlığı'nın Erişime Kapatıldığı An
Kaynak: Tarafımızdan ekran görüntüsü alınmıştır

3.29 2015 UKRAYNA ELEKTRİK KESİNTİSİ

23 Aralık 2015 saat 15:30'da Ukraynalıların Noel hazırlıkları yaptıkları esnada elektrik şebekesini kontrol eden SCADA sistemine siber saldırı olması sonucu elektrikler kesilmiş ve 30 yakın elektrik birimin kapatan saldırı sonucunda 250.000'e yakın Ukraynalı karanlığa gömülmüştür. Araştırmalar sonucunda hackerların saldırıya bahar aylarında phishing maili ile santral çalışanlarına virüs göndererek başladıkları tespit edilmiştir (Başaran, 2017, s:17-19).

3.30 2016 UKRAYNA ELEKTRİK KESİNTİSİ

23 Aralık 2015'te gerçekleşen saldırıdan tam bir yıl sonra 2016 Aralık ayında Ukrayna elektrik alt yapısı tekrar siber saldırıya uğramıştır. Bu seferki saldırı bünyesinde hackerlara hedef sisteme komut göndermelerini sağlayan bir bağlantı, saldırı kodu yüklenilmesini sağlayan bir modül ve çeşitli hazır saldırılar içeren "Crashoverride" adında bir virüs tarafından yapılmıştı. Ayrıca virüs hedef sistemlere bulaştıktan sonra komut beklemeden de görevini yerine getirecek şekilde tasarlanmıştı (Başaran, 2017, s:20).

2015'te yaşanan ve bir yıl sonra tekrar eden Ukrayna elektrik kesintisi saldırılarının en önemli etkileri saldırıların yapıldıkları tarihler açısından noel süsü satan firmaların zarar girmesi o tarihlerin reklam fiyat tarifeleri farklı olduğu için tv kanallarının zarara girmesi ve tekrar ettiği için insanların psikolojik olarak yıpranmalarıdır. Ayrıca bir diğer önemli ayrıntı ise saldırganların elekrtik tesistlerinin tasarımlarını en ince ayrıntılarına kadar ele geçirmiş olmasıdır. Saldırılarını otomatik hale geticerek kadar bilgiyi başka türlü edinemezlerdi.

3.31 2016 NEW YORK BORSASINA SALDIRI

Ünlü Türk hacker grubu Aslan Neferler Tim, bu defa New York Borsasını hedef aldı. Yurt içi ve yurt dışında ses getiren siber saldırılarda bulunan grup, New York borsasının sunucularını çökertti. ABD'nin, para için Müslümanlara zulüm yaptığını gerekçe gösteren grup üyeleri, ABD'yi maddi yönden zarara uğratmak için New York

borsasının işlem, data ve finans sunucularını çökertti. Grup, borsanın işlem hacimleri baz alındığında 800 milyon dolar zarara uğratıldığını kaydetti(http://www.milliyet.com.tr/gundem/turk-hackerlardan-new-york-borsasina-siber-saldiri-2350081 , 21.05.2019).

Bu saldırı hackerların veya hacktivistlerin hedefleme stratejilerini değiştirdiklerini, geliştirdiklerini göstermektedir. Eskisi gibi devlet kurumları yada rastgele siteler hacklemek yerine artık hackerlar da ekonomik açıdan değer arz eden hedefleri vurmaktadırlar.

3.32 2016 ABD-ÇİN-RUSYA SİBER SAVAŞI

Amerika Birleşik Devletleri tarihin en büyük siber saldırısı ile karşı karşıya kaldı. 21 Ekim Cuma günü başlayan saldırı Rus ve Çinli hackerlar tarafından ABD hedef alınarak 14 milyondan fazla IP üzerinden gerçekleştirildi. DDoS yani Distributed Denial of Service (Dağıtık Hizmet Engelleme) olarak adlandırılan bu saldırı türü internet sistemlerini engellemek için yapılıyor.

Bugün gelinen noktada ise FBI ve Pentagon bu saldırıları engellemek için dün erken saatlerden bu yana tüm çalışmalarına devam ediyor. Ancak henüz tatmin edici bir ilerleme kaydedilemediği belirtiliyor. Yani ABD'de tüm uğraşılara rağmen saldırının önüne geçilemediği gibi dünyanın yeni savaş silahı olarak nitelediği bu saldırıların Amerika'ya maliyeti ise belli olmaya başladı.

Başta ABD olmak üzere onlarca ülkenin etkilendiği DDoS atakları nedeniyle sadece sosyal medya siteleri değil DynDNS gibi dünyanın en büyük DNS servis sağlayıcısının yanı sıra mesajlaşma uygulaması WhatsApp, dijital oyun platformu Origin ve Steam de bu saldırıların hedefi oldu. Bunların dışında Amerikan hükümetine ait kurum ve kuruluşların sitelerinin de çöktüğü belirtiliyor. Teknoloji dünyasında yayılan söylenti ve paylaşımlara göre DDoS saldırısı Amerika'ya pahalıya patladı. Ülkenin yüzde 78'inden fazlasının internetsiz kaldığı belirtilirken maddi zararın ise 7 milyar doları bulduğu ifade ediliyor(https://www.takvim.com.tr/dunya/2016/10/22/siber-saldirinin-abdye-maliyeti-7-milyar-dolar, 21.4.2019). Yedi milyar dolar zarar yol açan bu saldırının dışsal ekonomik etkileri arasında günümüzde sıkça duyduğunuz Çin malı ürünlerin ABD'de

yasaklanması gibi pek çok yaptırımın ekonomik sonuçları gösterilebilir. Çünkü bu saldırılar Çin malı akıllı cihazlar üzerinden yapılmıştır.

3.33 2016 ABD SEÇİMLERİ

8 Kasım 2016 tarihinde gerçekleşen seçimlerden önce ABD başkan adayı Danold Trump Rus hackerlara çağrıda bulundu. Rus istihbaratının Demokratik Ulusal Komite'nin bilgisayar sunucularını hacklediğine ilişkin haberlere değinerek Demokrat Parti'nin başkan adayı Hillary Clinton'un silinmiş elektronik postalarının bulunması için Rus internet korsanlarına çağrı yaptı.

Bunun üzerine Hillary Clinton Rusya yı seçimlere müdahale etmekle suçladı.

Ve Rusya iddiaları reddetti.

Ancak NBC News kanalına konuşan Amerikan istihbarat yetkilileri, ABD Başkanı Barack Obama yönetiminin Rusya 'ya siber anlamda cevap verilebilmesi için CIA yetkililerine gerekli çalışmayı yapmaları talimatını verdiğini iddia etti.

Seçimler sonucunda Donald Trump seçildikten sonra da seçimlere Rusya'nın siber müdahalede bulunduğu iddialarının devam etmesi üzerine Donald Trump CIA direktörünü ve FBI başkanı James Comey'i görevden aldı.

3.34 2018 CATHAY PACİFİC HAVAYOLU ŞİRKETİNE SALDIRI

Cathay Pacific Havayolu'nun müşteri bilgileri internet korsanları tarafından çalındı. Yedi yıl sonra hacklendiğini fark eden Hong Kong merkezli şirket, 9.4 milyon müşterinin pasaport, kredi kartı, telefon numaraları, adres ve e-posta bilgilerine ulaşıldığını açıkladı. Şirkete göre, çalınan söz konusu bilgilerin kötü amaçlarla kullanıldığına dair henüz bir kanıt yok. Cathay Pacific'in hacklenmesi, havacılık sektöründe bugüne kadar yaşanan en geniş kapsamlı veri hırsızlığı olarak gösteriliyor. Skandalın ortaya çıkmasıyla Cathay Pacific borsada yüzde 6,5 büyüklüğünde değer kaybı yaşadı, bu 201 milyon dolara tekabül ediyor(http://www.milliyet.com.tr/dunya/unlu-havayolu-sirketi-hacklendi-2766944 , 26.4.2019). Cathay pasific firmasının yaptığı açıklama siber saldırıların etkilerini saklama refleksinin iyi örneklerinden birisidir. Bu

saldırı sonucunda elde edilen verilerle kimlik sahteciliği, bu verilerin çeşitli terör örgütü gruplarına satılması ve daha pek çok dışsal ekonomik sonuç meydana gelebilir. Siber saldırıların ekonomik etkilerini olduğundan daha az göstermeye çalışmak veya ciddiye almamak yanlış bir yaklaşımdır. Ayrıca müşterilerin çalınan verileri ulusal güvenlik açısından da sorun teşkil etmektedir. Ve son olarak olay sonucunda şirketin borsa da değer kaybetmesi de bu saldırının dışsal bir ekonomik etkisidir.

SONUÇ

Yaptığımız çalışmanın en önemli bulgusu siber saldırıların ekonomik boyutlarını hesaplamak üzere disiplinler arası bir sistematik geliştirilmesinin gerekliliğidir. Bu konudaki çözüm önerimiz çalışmanın birinci bölümünde yer alan yapay zekâ başlığı altındaki, yapay zekânın finansal uygulamaları alt başlığında vermiş olduğumuz örnekteki gibi bir yapay zekâ modeli kullanılarak, kurulan yapay zekâ modeline çeşitli disiplinlerce tespit edilen siber saldırıların ekonomik etkilerini hesaplamaya ilişkin değişkenlerin girilerek yapay zekânın öğretilmesidir.

Daha açıklayıcı olması açısından birinci bölümde bulunan savaş ve siber savaş ekonomisi başlığı altında siber güvenlik endeksi (GCI) kavramından ve bilişim teknolojileri gelişmişlik endeksi (IDI) kavramından bahsedilmektedir. Bu endeksler uzmanlarca belirli kriterlere ağırlıklı puanlar verilerek hesaplanmaktadır. Endekslerin değerleme tabloları da ilgili bölümde bulunmaktadır. Örneğin GCI endeksinin ağırlık tablosunda 0.032 ağırlık puanıyla bulunan Siber Güvenlik Mesleki Eğitim Kursları, kapasite geliştirme gibi çeşitli ağırlıklardaki kriterlerin de ağırlık puanları yapay zekâ ile modellenerek sınanmalıdır. Elde edilen sonuçlar doğrultusunda daha doğru ağırlık puanlarına ulaşılacaktır.

Diğer bir önemli nokta ise GCI ve IDI siber güvenliğe yönelik geliştirilmiş endekslerdir. Benzer şekilde siber saldırıların ekonomik etkilerinin daha iyi hesaplanabilmesi için Bilişim Etki Liste Endeksi (BELEN) endeksi veya başka bir isimle başka bir endeks geliştirilmelidir. Burada kavramsal açıdan BELEN endeksi olarak önerdiğimiz endeksteki liste kısmına; saldırıya uğrayan hedefin bulunduğu ekonomiye dair ekonometrik veriler, hedefin ekonomideki büyüklüğü, yer aldığı sektör, sektörün ülke ekonomisindeki ağırlığı, sektörün dış ticaretteki ağırlığı, saldırıya uğrayan hedefin bulunduğu ülkenin dünya ekonomisindeki ağırlığı, saldırıya uğrayan hedefin tedarikçi ve müşteri düzeyinde ilişkileri, kullanılan saldırı türü, GCI ve IDI endeksleri gibi daha pek çok ilgili veri eklenmelidir. Bu listeye eklenilmesi düşünülen veriler yapay zekânın finansal uygulamalarında şirketlerin muhasebe bilgilerini girerek şirketlerin gelecekteki durumlarını yüksek başarı oranıyla tahminledikleri örnekteki gibi, yapay zekâ modeline girilmeli ve siber saldırının ekonomik etkisi hakkında tahminlemeler yapılmalıdır. Yapay zekâ bu verileri işledikçe yıldan yıla daha doğru tahminleri ve bizim göremediğimiz

ilişkileri ortaya çıkaracaktır. Bu noktadan sonra da tespit edilen doğru ağırlık puanları ile gerçekten yatırım yapılması gereken önleme yöntemleri ortaya çıkacaktır.

Ülkemiz açısından bu önerimizin önemi ise; Türkiye, bölgesinde yapay zekâ konusunda lider bir ülkedir. Önerdiğimiz şekilde geliştirilen bir yapay zekâ modelinden elde edilecek veriler ekonomimize ciddi katkılar sağlayacaktır. Bunun daha iyi anlaşılması açısından nasıl ki Uluslar Arası Polis Gücü (INTERPOL), Kaspersky firması ile siber tehdit istihbaratı antlaşması yaptıysa önerilen çalışmanın hayata geçirilmesi durumunda da Türkiye bu konuda lider olacaktır. Bunun sonucunda da siber güvenlik sigortası değerleme, bilişim teknolojileri geliştirme stratejileri, siber güvenlik yatırım kararı ve stratejileri gibi pek çok konuda Türkiye, dünya çapında bir otorite olacaktır.

Önerilerimiz dışında elde ettiğimiz diğer bulgular şu şekildedir:

Gelişen teknoloji ile birlikte ekonomik tercihler, ödeme araçları ve politika araçları da değişti. Günümüzde e-ticaret ekonominin önemli bir paydasını oluşturmakta.

Siyasi politikalar artık sosyal medya üzerinden lanse ediliyor. Medya yerini yavaş yavaş siber dünyaya bırakıyor. Ödemelerimizin ve alışverişlerimizin azımsanmayacak bir kısmı internet üzerinden yapılıyor. Ekonomik malların ve hizmetlerin üretiminden satışına kadar her aşamasında elektronik sistemler gittikçe daha çok kullanılıyor.

Pratiklik açısından pek çok kolaylık getiren bu sistemler birçok tehlikeyi de beraberinde getiriyor. Teknolojinin gelişmesi ile bu sistemlerin kullanımının artması da artık kaçınılmaz bir hal aldı. Ve tabi bununla birlikte ortaya çıkacak risklerin artmasının da kaçınılmaz olduğunu öngörmek zor değil.

Gün geçtikçe her alanda daha çok sanallaşıyoruz. Hatta artık savaşlar dahi internete taşındı, siber güç savaşların ve iç çatışmaların önemli bir cephesi haline geldi.

İstihbarat artık insan merkezli olmaktan çok sosyal ağlar ve bilişim sistemleri üzerinden elde ediliyor. Aslında NSA, ECHELON gibi bazı kurumlar bunu yıllardır yapıyorlar.

Tabletleriniz bilgisayarlarınız telefonlarınız, yazıcılarınızdaki çipler ve hemen hemen her türlü internet erişimi olan akıllı ürünler gerektiğinde bir istihbarat kaynağı ve gerektiğinde bir siber saldırı aracı olarak kullanılabiliyor.

Bunu sadece ismini andığımız kuruluşlar yapmıyor siber alemin önemli aktörleri olan hacker diye tabir edilen kişi veya gruplarda bu sahnede önemli bir rol oynayan aktörler.

Amerika tarafından hazırlandığı düşünülen Stuxnet isimli virüsün İran'ın uranyum zenginleştirme programını tam iki yıl sekteye uğratması;

Arkasında Çin'in olduğu düşünülen flame virüsü, titan rain virüsü gibi birçok farklı virüsler ile küresel ölçekte endüstriyel casusluk yapıldığının ortaya çıkması;

Kısa bir süre önce koalisyon güçleri ile Musul'u DEAŞ terör örgütünden arındırmak için yapılacak olan operasyon planlarını DAEŞ in hack yoluyla ele geçirmesi;

İnternetin karanlık yüzü olan Darknet ten DAEŞ in biyolojik silah malzemeleri temin etmesi;

ABD'nin Irak savaşından önce Irak ordusunun askeri ağına sızarak Irak askerlerini teslim olmaya ikna etmesi;

Geçtiğimiz Amerikan seçimleri öncesinde Rus hackerler tarafından başkan adayı olan Clinton' ın partisinin, internet sitesinin hacklenmesi;

Bunun akabinde ABD'nin Rusya'yı siber savaş la tehdit etmesi ve Rus hackerların buna sessiz kalmayıp Amerika ya tarihin en büyük D-DOS saldırısını gerçekleştirmesi sonucu Amerika'nın 7 milyar dolar zarar uğraması.

Detaya indiğimizde sessiz tehlikeyi duymak mümkün. Detaya indiğimiz de Amerika ya yapılan saldırıda ev aletleri ve günlük kullanım için olan birçok akıllı ürünün veri trafiği kullanılarak bu saldırının yapıldığı gerçeği, tehlikenin evlerimize kadar girdiğini anlamamıza yeter sanırım.

Saydığımız bu örnekler dışında da daha pek örnek olay sıralayabiliriz.

Bütün bunları ve siber güvenliğin NATO gündemine alınmasını dikkate aldığımızda sosyal medya iletişim ve siber savaşların küresel ölçekte politik, ekonomik, stratejik anlamda ve daha pek çok açıdan ne denli önemli bir rol oynadığını ve kritik öneme sahip olduğunu anlıyoruz.

Bu tehlikelerin ekonomik boyutlarını ortaya koymak açısından disiplinler arası ampirik bir çalışma yapmak faydalı olacaktır.

Anlatılan saldırı teknikleri ve örnek saldırıların sonuçları göz önünde bulundurulduğunda seçilen saldırı tekniği ve saldırıdan sonra geçen zamana bağlı olarak saldırının ekonomik boyutları da artmaktadır.

Bunu bir salgın gibi düşünebiliriz örnek vermek gerekirse Stuxnet virüsü aylarca siber uzayda dolandı ama hedefine ulaşana kadar herhangi bir zarar yol açmadı.

Fakat hedefe ulaştıktan sonra nükleer santralin çalışmasını engelledi ve nükleer santralin devre dışı kalmasına yol açtı.

Bu tür tesislere yapılan saldırıların ekonomik zarar skoruna ilk etkin olduğu anda nükleer santralin maliyetini ilerleyen anlarda ise nükleer santralden elektrik alan ve ekonomik anlamda faaliyette bulunan fabrikaların ve bireylerin ekonomik zararlarını ve daha da ilerleyen zamanda bu olaydan borsa da etkilenen firmalar varsa onların değer kayıplarını devletin bu saldırının etkilerini bertaraf etmek ve araştırmak için yaptığı araştırma maliyetlerini zincirleme şekilde eklersek ekonomik anlamda ne denli bir etkiye yol açıldığını betimsel olarak anlatmış oluruz.

Tabi ki gene belirttiğimiz gibi bunun ampirik çalışmasını yapıp sayısal rakamlara dökmek ve bir ilişki kurmak başka bir araştırmanın konusu olacaktır.

Üç boyutlu yazıcılarla araba üreten veya kullanım için eşyalar üretenler olduğu gibi günümüzde artık bu teknolojilerle silah üretimi de yapılmaktadır. Siber saldırıların artması ile birlikte her endüstrinin etkilendiği gibi savaş endüstrisinin de etkilendiğini söylemek mümkündür. NATO'nun ve ABD'nin savaş stratejilerinde kara, deniz, hava ve uzaydan sonra siber âlem beşinci savaş bölgesi olarak yer almaktadır. Fakat sıralama bizi yanıltmamalı beşinci savaş bölgesi olması tamamen yeni açılan bir cephe olduğu içindir. Önem sırasında birçok uzmana göre birinci sırada gelir, hepsinden önceliklidir, siber savaşlar gerçektir ve siber savaşlar bütün diğer savaş alanlarını kapsamaktadır. Günümüzde artık hemen her devlet hacker orduları kurmaktadır. ABD, İran ve Kuzey Kore'nin binlerce kişiden oluşan hacker orduları bulunmaktadır. ABD gibi devletlerde bu tür savaşlar NSA veya ECHELON gibi kurumlar üzerinden sistematik olarak yürütülmektedir. Akerlof'un "Limon Piyasalar" asimetrik bilgi kuramı NSA in ekonomik fonksiyonunu iyi açıklayabilecek bir kuramdır. Akerlof'a göre limon olarak tabir ettiği sorunlu ikinci el arabalardır ve satıcılar bu arabaların gerçek değerini bilirken alıcı sadece fiyatını bilmektedir. Boing firmasının 1993 yılında Suudilerle yaptığı görüşmeleri NSA'in dinlemeleri sonucu kazandığı artık herkesçe biliniyor. Yani bu tür siber istihbarat sistemleri bulunan ülkelerin diğerlerine nazaran bir asimetrik bilgi, limon piyasa modeli oluşturduğunu söylemek yanlış olmayacaktır. Bu yolla kendi şirketlerini rakiplerinin

önüne geçirdikleri de bilinen bir gerçektir. Fakat en başında belirttiğimiz gibi bu tür zararların etkilerini net olarak hesaplamak oldukça güçtür çünkü bahsettiğimiz üzere bu bir çeşit savaş ekonomisidir ve zararları gerçektir.

KAYNAKÇA

Ada, M. & Çakır, H. (2017). "*Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi"* Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 638.

Akar, Gökhan (2015), *"Nükleer Tesislerde Bilişim Eemniyeti"* Yayınlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Enerji Enstitüsü, İstanbul.

Akbulak, Sevinç& Akbulak, Yavuz, Marmara Üniversitesi, İ.İ.B.F Dergisi, Yıl 2008, Sayı 2, s 243

Aksoy, Emre (2018), *Bitcoin Paradan Sonraki En Büyük İcat*, 1, Abaküs Yayınları: İstanbul

Aktaş, Onur (2017), *Siber Güvenlik-Hacking-Atölyesi*, Gazi Kitabevi: Ankara

Alçelik, Aykut (2017), *Google Adwords*, 2, Dikeyeksen Yayınları: İstanbul

Alican, Fuat (2006*), Ekonomik Ve Sosyal Boyutlarıyla Dünyada Ve Türkiye'de Yazılım Sektörü*, 1, İletişim Yayınları: İstanbul

Altınkaynak, Mustafa (2017), *Uygulamalı Siber Güvenlik Ve Hacking*, 3, Abaküs Yayınları: İstanbul

Altınok, Besim (2017), *Kablosuz Ağ Güvenliği (Saldırı, Savunma, Analiz)*, 1, Abaküs Yayınları: İstanbul

Altuntaş, Abdülaziz (2017), *Metasploit Ve Penetrasyon Testleri*, 4, Kodlab Yayınları: İstanbul

Aydın, Orhan (2013), *Yapay Zekâ: Bütünleşik Bilişe Doğru*, İstanbul Gelişim Üniversitesi Yayınları: İstanbul

Aytekin, Akın, (2015), "*Türkiye'nin Siber Güvenlik Stratejisi Ve Eylem Planının Değerlendirilmesi"*, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Bakoğlu, H. (1975). "*Algol Programlama Dili*", İstanbul: İstanbul Teknik Üniversite Matbaası

Bartlett, Jamie (2016), *Dark Net İnternetin Karanlık Dünyası*, (Çev. Yasin Konyalı), 1,Timaş Yayınları: İstanbul

Başaran Alper (2017), *Siber Kıyamet*, 1, Arion Yayınları: İstanbul

Bayraktar, Gökhan (2015), *Siber Savaş Ve Ulusal Güvenlik Stratejisi*, Yeniyüzyıl Yayınları: İstanbul

BBC, "*Estonia hit by 'Moscow cyber war'"* [Erişim: 9.7.2019, http://news.bbc.co.uk/2/hi/europe/6665145.stm]

Bilgi Güvenliği Akademisi, "*Sızma Testi*", [Erişim: 5.05.2019 https://www.bgasecurity.com/danismanlik-hizmetleri/penetrasyon-testi-sizma-testi]

Bodur, Hüseyin (2016), *Java Diliyle Kriptoloji Uygulamaları*, 1, Abaküs Yayınları: İstanbul

Bozkurtlar, Burak (2017), *Anne Ben Hacker Oluyorum*, 1, İkinci Adam Yayınları: İstanbul

Bölükbaş, Yunus (2017), *Wireshark İle Network Analizi*, 1, Dikeyeksen Yayınları: İstanbul

Bülbül, İsmail Ve Bingöl, Poyraz Emre (2017), *Etik Hackerlığa Giriş*, Hayygrup Yayıncılık: İstanbul

CEİCData, *"Countries External Debt"*, [Erişim: 1.7.2019 www.ceicdata.com/en/indicator/external-debt]

Clarke, Richard Ve Knake, Rorbert (2011), *Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit*, (Çev. Murat Erduran), İstanbul Kültür Üniversitesi Yayınevi: İstanbul

CNN Türk, "*Bilgisayar virüsü Atatürk Havalimanı'nı Felç Etti*" [Erişim: 9.7.2019, https://www.cnnturk.com/2009/bilim.teknoloji/teknoloji/01/30/bilgisayar.virusu.ataturk.havalimanini.felc.etti/511371.0/index.html]

Critical Infrastructure Protection Vıgılance, "*A Shortlist of Reported SCADA Incidents*" [Erişim:08.07.2019 https://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/]

Çakmak, Haydar Ve Altunok, Taner (2009), *Suç, Terör Ve Savaş Üçgeninde Siber Dünya*, Barış Platin Yayınları: Ankara

Çelik, M. K. (2010). *"Bankaların Finansal Başarısızlıklarının Geleneksel Ve Yeni Yöntemlerle Öngörüsü"* Yönetim Ve Ekonomi, 142.

Çıtak, Ömer (2018), *Ethical Hacking*, 1, Abaküs Yayınları: İstanbul

Çifci, Hasan (2017), *Her Yönüyle Siber Savaş*, 2, TÜBİTAK Yayınları: Ankara

Domingos, Pedro (2017), *Master Algoritma – Yapay Öğrenme Hayatımızı Nasıl Değiştirecek?*, (Çev. Tufan Göbekçin), 2, Paloma Yayınevi: İstanbul

Eczacıbaşı, Faruk (2018), *Daha Yeni Başlıyor: Geleceğin Dünyasında Esneklik, Yakınsama, Ağ Yapışı ve Karanlık Taraf*, 1, Koç Üniversitesi Yayınları: İstanbul

Elbahadır, Hamza (2017), *Hacking İnterface*, 16, Kodlab Yayınları: İstanbul

Eren, Mehmet (2017), *Avrupa Birliği'nin Siber Güvenlik Politikası*, Beta Yayınları: İstanbul

Ertem, C., & Uçkan, Ö. (2011),"*Wikileaks Yeni Dünya Düzenine Hoş Geldiniz*" İstanbul: Etkileşim Yayınları.

Esenyurt, *"binary sistem",* [Erişim: 6.7.2019, https://www.buraksenyurt.com/post/Decimal-to-Binary-to-Hexadecimal]

Flowler, Zoe (23.4.2013), *"Who is the Syrian Electronic Army?",* BBC, [Erişim: 1.07.2019, https://www.bbc.com/news/world-middle-east-22287326]

Gertner, J. (2013), *Fikir Fabrikası Bell Laboratuvarları Ve Amerikan Yenilikçiliği'nin Altın Çağı",* İstanbul: Modus Kitap.

Gibson, William (2003), *Neuromancer*, (Çev. Petek Demir & İpek Demir), Altın Kitaplar Yayınevi: İstanbul

Global Fire Power 2019, *"Ülkelerin Ateş Gücü Sıralaması"*, [Erişim: 20.06.2019 https://www.globalfirepower.com/countries-listing.asp]

Global Security, "*Solar Sunrise*" [Erişim: 07.07.2019 https://www.globalsecurity.org/military/ops/solar-sunrise.htm]

Goodman, Marc (2016), *Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü*, (Çev. Yavuz Türk), 1, Timaş Yayınları: İstanbul

Gökdemir, Orhan (2013), *RedHack*, 7, Destek Yayınları: İstanbul

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

Habertürk, *"Siber Korsanlar 4000 Siteye İzinsiz Madencilik Yapan Zararli Yazilim Yerlestirdi"* [Erişim:1.5.2019, https://www.haberturk.com/siber-korsanlar-4000-siteye-izinsiz-madencilik-yapan-zararli-yazilim-yerlestirdi-1834257-ekonomi]

Henkoğlu, Türkan (2014), *Adli Bilişim*, 2, Pusula Yayınları: İstanbul

Hootsuite (2018), Simon Kemp, *Digital in 2018 Global Overview*, *Ülkelerin Sosyal Medya Erişim Oranları*, [Erişim: 1.7.2019 https://wearesocial.com/blog/2018/01/global-digital-report-2018] S:54

Hootsuite (2018), Simon Kemp, *Digital in 2018 Global Overview*, *Ülkelerin İnternet Erişim Oranları*, [Erişim: 1.7.2019 https://wearesocial.com/blog/2018/01/global-digital-report-2018] S:31

Hootsuite (2018), Simon Kemp, *Digital in 2018 Global Overview*, *Ülkelerin Facebook Kullanım Oranları*, [Erişim: 1.7.2019 https://wearesocial.com/blog/2018/01/global-digital-report-2018] S:73

Hootsuite (2018), Simon Kemp, *Digital in 2018 Global Overview*, *Ülkelerin İnstagram Kullanım Oranları*, [Erişim: 1.7.2019 https://wearesocial.com/blog/2018/01/global-digital-report-2018] S:76

IBM, *"Binary Table",* [Erişim: 6.7.2019, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ioaq100/ascii_table_appendix.htm]

Interactive Advertising Bureau Türkiye (2018), *2018 Dijital Reklam Yatırımları*,(AdEx-TR 2018). [Erişim:1.7.2019 http://www.iabturkiye.org/UploadFiles/Adex/infografik_15.04.19(1)1642019100030.pdf].

International Telecommunication Union (ITU), "*Ülkelerin Küresel Siber Güvenlik Endex Puanları"* Global Cybersecurity Index 2018

International Telecommunication Union(ITU), *Bilişim Teknolojileri Gelişmişlik Endeksi (IDI) Ve Küresel Siber Güvenlik Endeksi (GCI)* Global Cybersecurity Index 2018

Kahraman, Benan (2016), *Bilinmeyen Bilişim*, 1, Meta Yayınları: İzmir

Kaliç, Sabri (2012), *Anonymous Sanal Âlemin Korsanları*, 1, Maya Yayınları: İstanbul

Kara, Mahruze (2013), *Siber Saldırılar - Siber Savaşlar Ve Etkileri* Yayınlanmamış Yüksek Lisans Tezi İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Kaya, Adem (2012), "*Siber Güvenliğin Milli Güvenlik Açısından Önemi"*, Yayınlanmamış Yüksek Lisans Tezi, T.C. Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara.

Keleştemur, Atalay (24.2.2109), *"EC-Council Hacklendi, Kimlikler İfşa Edildi!"*, h4cktimes, [Erişim: 5.1.2019, https://h4cktimes.com/siber-saldirilar-suclar/etik-hacker-kurulusu-ec-council-hacklendi-edward-snowdenin-pasaportu-yayinlandi.html]

Kleinman, Zoe (2.3.2016), "*Akıllı telefonlarınız sizi dinliyor olabilir*", BBC, [Erişim: 1.7.2019, https://www.bbc.com/turkce/haberler/2016/03/160302_casus_akilli_telefon]

Kurtoğlu, Ramazan (2017), *Küresel Para Oyunları Ve Psiko-Siber Savaş*, Destek Yayınları: İstanbul

Meral, Mustafa (2015), "*Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi*", Yayınlanmamış Yüksek Lisans Tezi, T.C. Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul.

Milliyet, (20.10.2017), *"Ünlülerin Sosyal Medya Hesapların Çalan Türk Çetesi Yakalandı",* [Erişim: 1.7.2019, http://www.milliyet.com.tr/teknoloji/teknoloji-haberleri/spotifydan-disneye-ozel-calma-listesi-6002576]

Milliyet, "*Siber İntifada*" [Erişim:8.7.2019, *http://www.milliyet.com.tr/dunya/siber-intifada-5335183]*

Milliyet, "*Sosyal Medya Hesaplarını Çalan Türk Çetesi Yakalandı*", [Erişim: 1.07.2019, http://www.milliyet.com.tr/teknoloji/unlulerin-sosyal-medya-hesaplarin-calan-turk-cetesi-yakalandi-2540797]

Misner, P. (2019, 7 5), *Microsoft's Top 100 Security Researchers – Black Hat 2018 Edition Microsoft,* [Erişim: 1.07.2019, Https://Blogs.Technet.Microsoft.Com/Msrc/2018/08/08/Microsofts-Top-100-Security-Researchers-Black-Hat-2018-Edition/]

Mitnick, Kevın D. Ve Simon, William L. (2016), *Sızma Sanatı*, (Çev. Emel Aslan), 3, ODTÜ Yayıncılık: Ankara

Mitnick, Kevın D. Ve Simon, William L. (2017), *Aldatma Sanatı*, (Çev. Nejat Eralp Tezcan), 1, ODTÜ Yayıncılık: Ankara

Murchu, Liam (25.7.2010), *"W32.Stuxnet – Network Operations",* Symantec, [Erişim: 9.7.2019, https://www.symantec.com/connect/blogs/w32stuxnet-network-operations]

National Security Archive, *"Eligible Receiver 97: Seminal DOD Cyber Exercise Included Mock Terror Strikes and Hostage Simulations"* [Erişim: 07.07.2019 https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-01/eligible-receiver-97-seminal-dod-cyber-exercise-included-mock-terror-strikes-hostage-simulations]

NTV, *"Kızıl Hackerlar Polis Sistemini Hackledi",* [Erişim: 1.7.2019, https://www.ntv.com.tr/turkiye/kizil-hackerlar-polis-sistemini-hackledi,3w7o4PZrQUaj55JEzb2NRA?_ref=infinite]

Olson, Parmy (2014), *Biz Anonymous 'uz*, (Çev. Suphi Nejat Ağırnaslı), Paloma Yayınevi: İstanbul

Ponemon Enstitüsü & Accenture Siber Güvenlik 2019 Siber Suç Maliyet Raporu, "*Doğrudan ve Dolaylı Siber Saldırıların Riske Attığı Değer Sonraki 5 yıl için tahminleme (Birikimli 2019-2023)"* [Erişim: 24.06.2019 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50]

Reel Dünyada Sanal Açmaz Siber Alanda Uluslararası İlişkiler, (2011), Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, 271.

Ronfeldt,, D., & Arquilla, J. (2001), *"Networks And Netwars The Future Of Terror, Crime, And Militancy"*. Usa: Rand Corporation.

Singer, Peter Warren (2015), *Robotik Savaş 21. Yüzyıldaki Robotik Devrim*, (Çev. Murat Erdemir, Tüba Erem Erdemir), Buzdağı Yayınevi: Ankara

Singer, Peter Warren Ve Friedman, Allan (2015), *Siber Güvenlik Ve Siber Savaş*, (Çev. Ali Atav), 1, Buzdağı Yayınevi: Ankara

Statista, "*Nvidia-And-Radeon-Gpu-Pricing*" [Erişim: 6.7.2019, https://www.statista.com/chart/15843/nvidia-and-radeon-gpu-pricing/]

Statista, "*FaceApp Kullanımı"*, https://www.statista.com/chart/18769/estimated-worldwide-faceapp-downloads-by-platform/ , [Erişim:21.07.2019]

Sunn, Frank (2001), *Canavarın İnternetteki Sayısı:666*, (Çev. Özgül Erman), Cep Yayıncılık: İstanbul

Şahin, Tamer (2012), *Hacker'ın Aklı Türkiye'nin İlk Bilgisayar Korsanının Anıları*, 1, Doğan Yayıncılık: İstanbul

Şahinaslan, Önder, (2013),"*Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu Ve Çözümü Üzerine Bir Çalışma"*, Yayınlanmamış Doktora Tezi, T.C. Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Taner, Cemal (2018), *Kali İle Ofansif Güvenlik*, 1, Abaküs Yayınları: İstanbul

Taşkın, Deniz (2012), *Gömülü Sistem Tasarımı*, 1, Papatya Yayınları: İstanbul

Tuncer, Emre (2014), *Sosyal Medya İmparatorluğu-Patron*, 1, Akis Yayınları: İstanbul

Türk Dil Kurumu (2019), "*Bilim ve Sanat Terimleri",* [Erişim: 1.7.2019, http://sozluk.gov.tr].

Türkiye Bilimler Akademisi (2019) *Bilim ve Sanat Terimleri,* [Erişim: 1.07.2019 www.tubaterim.gov.tr]

Usta, A. (2019, 7 1), "*Bankalar Arası Kart Merkezi Bankalar Arası Kart Merkezi*": Https://Www.Bkm.Com.Tr/Wp-Content/Uploads/2018/06/Paranın-Serüveni-2.-Baskı.Pdf Adresinden Alındı

Ünal, Naci (2015), *Siber Güvenlik Ve Elektronik Bileşenleri*, Nobel Yayınları: Ankara

Ünsal, E, Kocaoğlu, Ö. (2018),"*Blok Zinciri Teknolojisi: Kullanım Alanları"*, Açık Noktaları ve Gelecek Beklentileri. Avrupa Bilim ve Teknoloji Dergisi, (13), 54-64. DOI: 10.31590/ejosat.423676

Ünsal, Ersin Ve Kocaoğlu Ömer, (2018), "*Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri"* [Elektronik Sürüm], *Avrupa Bilim ve Teknoloji Dergisi*, (13): S:55, ss. 54-64

Vigna, Paul Ve Casey, Michael (2017), *Kriptopara Çağı Bitcoin ve Dijital Paranın Küresel Ekonomik Sisteme Meydan Okuması*, (Çev. Ali Atav), 1, Buzdağı Yayınevi: Ankara

Weill. Peter Ve Broadbent, Marianne (1999), *Şirketler İçin Yeni Bir Kaldıraç Enformasyon Altyapısı*, (Çev. Ayfer Gündal Ünal), Boyner Holding Yayınları: İstanbul

Yalçınkaya, Mehmet Ali ve Küçüksille, Ecir, Uğur (2017), *Tam Kapsamlı Sanal Test Laboratuvarı Kurulumu Ve Uygulamalı Sızma Testleri*, Abaküs Yayınları: İstanbul

Yıldız, Birol (2009), *Finansal Analizde Yapay Zekâ*, 1, Detay Yayıncılık: Ankara

ÖZGEÇMİŞ

Adı Soyadı: İbrahim ÖZKAN

Tel: 0551 621 33 44

Doğum Tarihi: 04.01.1990

Doğum Yeri: Bilecik/ Merkez

Lisans: Afyon Kocatepe Üniversitesi

Yüksek Lisans: Bilecik Şeyh Edebali Üniversitesi

Tez Konusu: Siber Saldırıların Ekonomik Boyutu

4 Ocak 1990 Bilecik doğumluyum. Lisans eğitimimi Afyon Kocatepe Üniversitesinde İktisat üzerine tamamladım. Yüksek lisans eğitimimi Bilecik Şeyh Edebali Üniversitesi'nde İktisat üzerine yapmaktayım. Gönüllü olarak Bilecik Edebalı Kültür ve Araştırma Derneği'nde yönetim kurulu üyesi olarak görev yapmaktayım. Aynı zamanda AFAD'a bağlı Edebalı Arama Kurtarma Derneği (EDAK)'ta gönüllü olarak görev yapmaktayım.