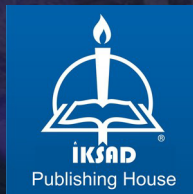


# KÜRESELLEŞME VE İNTERNET PARALELİNDE TERÖRİZMİN SİBER TERÖRİZME EVRİMİ

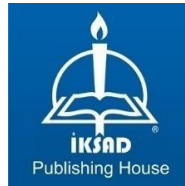
Mehmet SEĞMENOĞLU



# KÜRESELLEŐME VE İNTERNET PARALELİNDE TERÖRİZMİN SİBER TERÖRİZME EVRİMİ

**Mehmet SEĖMENOĖLU**

**Ankara – 2021**

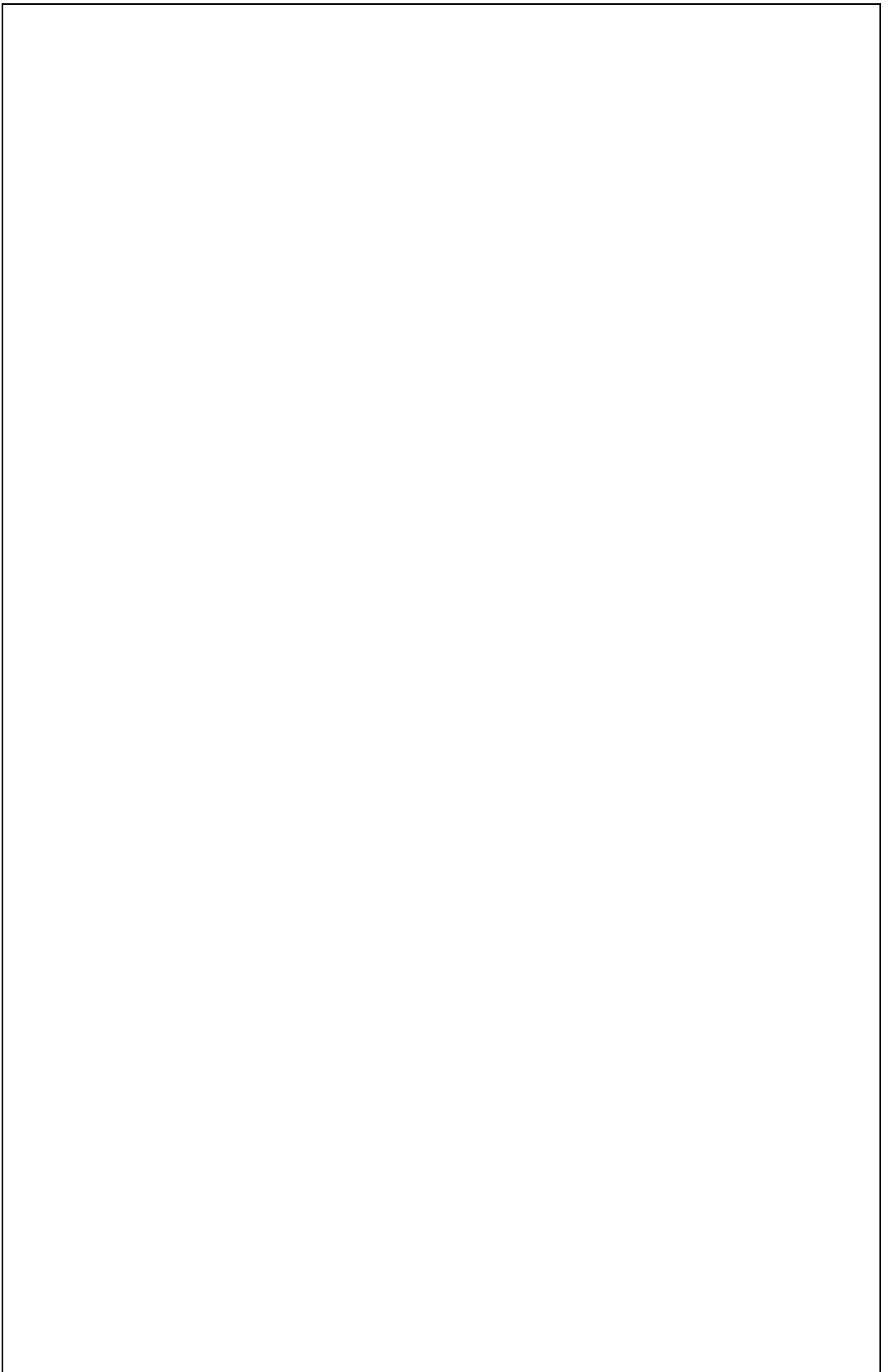


Copyright © 2020 by iksad publishing house  
All rights reserved. No part of this publication may be reproduced,  
distributed or transmitted in any form or by  
any means, including photocopying, recording or other electronic or  
mechanical methods, without the prior written permission of the  
publisher, except in the case of  
brief quotations embodied in critical reviews and certain other  
noncommercial uses permitted by copyright law. Institution of  
Economic Development and Social  
Researches Publications®  
(The Licence Number of Publicator: 2014/31220)  
TURKEY TR: +90 342 606 06 75  
USA: +1 631 685 0 853  
E mail: iksadyayinevi@gmail.com  
www.iksadyayinevi.com

It is responsibility of the author to abide by the publishing ethics  
rules.

Iksad Publications – 2021©  
**ISBN: 978-625-7636-76-6**  
Cover Design: İbrahim KAYA  
May / 2021  
Ankara / Turkey  
Size = 16 x 24 cm

*Varlıklarıyla bana daima güç veren ve desteklerini hiçbir zaman esirgemeyen eşim Şule ve oğlum İbrahim Ayaz'a sonsuz sevgilerimle...*



## **ÖNSÖZ**

Terör örgütleri, gerçek dünyada yüksek maliyetler ile gerçekleştirdiği terör eylemlerini, küreselleşmenin imkânlarını, bilişim ve iletişim ağlarını kullanarak çok az maliyetle çok büyük tahribatlar yaratabileceklerinin farkına varmışlardır. Bilişim, iletişim ve ulaşım teknolojilerindeki hızlı gelişmeler ile birlikte bir anlamda ulus devletlerarasındaki sınırların ortadan kalkması geleneksel anlamda ulus devletlerin sınırlarını kontrol etmesini ve denetim altına almasını güçleştirmiştir. Dolayısı ile her daim tetikte bekleyen terör örgütleri gerekli şartları sağladıklarında bu açıkları kendi çıkarlarına kullanacak şekilde eyleme geçmektedir. Ayrıca, terör örgütleri internet sayesinde propagandalarını çok daha kolay bir şekilde dünyaya yayabilmekte, kendine yeni sempatanlar bulabilmekte, örgütlenme ve eğitim programlarını çok kolay bir şekilde organize edebilmekte ve bunların hepsini neredeyse sıfır maliyet ile gerçekleştirebilmektedir. Bu anlamda siber terörün klasik terör anlayışından farklı özelliklere ve sonuçlara sahip olduğu değerlendirilmektedir.

Günümüzde teknolojinin olanakları sayesinde küreselleşmenin tüm dünya ülkelerini içine almaya başlaması devletlerin güvenlikleri için ciddi bir risk ortamı oluşturmaktadır. Tüm verilerin ve uygulamaların dijitalleşmesi sonucunda devletler siber uzaya bağımlı hale gelmektedirler. Bu bağımlılığın sonucunda ortaya çıkan risk, simetrik ve tek boyutlu olmanın aksine, asimetrik ve çok boyutludur. Bu bağlamda tüm dünyada düşman tanımından tehdit algılamalarına değin önemli farklılaşmalar yaşanmaktadır. Bu değişimler paralelinde

teröristlerin de eylemlerini gerçekleştirebilmek için patlayıcılara, hava taşıtlarına, silahlı gruplara ve bunları satın alabilmek için yüksek değerde mali kaynaklara olan ihtiyaçları azalmaktadır. Çünkü teröristler siber uzay platformunda siber terör eylemleri sonucunda da toplumda klasik terör eylemlerinde olduğu gibi korku ve dehşet ortamı oluşturmakta, dolayısı ile amaçlarına kolay yoldan ulaşabilmektedirler. Örneğin, teröristler bilişim ve iletişim sistemlerini hekeleyerek hedef ülkenin enerji sistemlerinin faaliyetini engelleyebilmekte, baraj kapaklarını kapatıp açabilmekte, hava trafik ve uçuş kontrol sistemlerini hekeleyerek uçak kazalarına neden olabilmektedirler. Hatta daha da hayalî olarak teröristlerin gıda üreten fabrikaların üretim sistemlerini hekeleyerek ürünlerin karışım oranlarını kendi amaçları doğrultusunda değiştirebilecekleri ve böylece kitlesel ölümlere yol açabilecekleri ihtimal dâhilindedir. Bu bağlamda siber terör eylemlerinin ülke güvenliğinden, halk sağlığı, ekonomi, politika, siyaset, halk refahı, hava, kara ve deniz trafiği ve diplomasinin örtülü faaliyetlerle desteklenmesine kadar geniş bir alanı etkilediği değerlendirilmektedir.

Bu kitapta sırasıyla “küreselleşme”, “internet” ve “terörizm” kavramları literatür taranarak açıklanmış ve sonrasında küreselleşmenin internetin gelişimi ile terörist eylemlerin siber uzayda etkinliğini artırmasına olan olası etkileri üzerine odaklanılmıştır. Çalışmada üç kavramsal zemin açıklandıktan sonra siber terörizmin alt başlıkları olan siber suç, siber terör, siber savaş kavramları ayrıntılı olarak ele alınmıştır.

## İÇİNDEKİLER

<b>ÖNSÖZ</b> .....	<b>I</b>
<b>İÇİNDEKİLER</b> .....	<b>III</b>
<b>KISALTMALAR</b> .....	<b>VII</b>
<b>TABLolar</b> .....	<b>IX</b>
<b>ŞEKİLLER</b> .....	<b>X</b>
<b>RESİMLER</b> .....	<b>XI</b>
<b>GİRİŞ</b> .....	<b>13</b>
1. Kitabın Amacı .....	13
2. Kitabın Önemi .....	135
<b>BİRİNCİ BÖLÜM</b>	
<b>KÜRESELLEŞME KAVRAMI</b> .....	<b>15</b>
1. Küreselleşme Öncesi Dünya Düzeni: Monarşiler ve Ulus Devletler ...	15
2. Uluslararasılaşma ve Küreselleşme .....	17
a. Lisans Anlaşmaları .....	20
b. Franchising Anlaşmaları .....	20
c. Ortak Girişimler .....	20
ç. Yeni İşletme Kurma veya Satın Alma.....	21
3. Teknolojik Gelişmenin Küreselleşmeye Etkisi .....	24
4. Küreselleşmenin Askeri Yönü .....	26
5. Küreselleşmenin İktisadi Yönü.....	28
6. Küreselleşmenin Sosyal Yönü.....	29
7. İletişim Araçlarının Küreselleşmeye Etkisi .....	30
<b>İKİNCİ BÖLÜM</b>	
<b>TOPLUM İLETİŞİMİNDE YENİ BİR ARAÇ: İNTERNET</b> .....	<b>32</b>
1. İnternet Nedir? .....	32
2. İnternette Erişim Nasıl Olur?.....	35
3. İnternet Güvenliği.....	36



4. Terör Bağlamında Medya ve Sosyal Medya ..... 39

## ÜÇÜNCÜ BÖLÜM

### TERÖR VE TERÖRİZM ..... 42

1. Geleneksel Terör ve Terörizm Kavramları ..... 42

2. Terör Örgütleri ve İnternet ..... 45

3. Terör Örgütlerinin İnternet Kullanımı ..... 47

a. İnternet Üzerinden Terör Saldırıları ..... 50

b. Terör ile Bağlantılı İçerikler ..... 54

(1) Terörist Bakış Açısının Sunumu ..... 54

(2) Terör Örgütlerinin Tehdit ve Propaganda Aracı Olarak İnternet . 58

(3) Terör Örgütlerinin Finansman Aracı Olarak İnternet..... 59

(4) Terör Örgütlerinin Örgüte Yeni Üye Alma Aracı Olarak İnternet 60

## DÖRDÜNCÜ BÖLÜM

### SİBER GÜVENLİK VE SİBER TERÖRİZM ..... 63

1. Siber Güvenlik ..... 65

2. Siber Eylem Sınıfları ..... 67

a. Siber Suç..... 68

(1) Bilgi ve Veri Aldatmacası (Data Diddling)..... 71

(2) Salam Tekniği (Salami Techniques)..... 71

(3) Süper Darbe (Super Zapping) ..... 71

(4) Eşzamansız Saldırıları (Asynchronous Attacks) ..... 72

(5) Truva Atı (Casus Yazılımlar) ..... 72

(6) Zararlı Yazılımlar (Malicious Software)..... 72

(7) Mantık Bombaları (Logic Bombs)..... 72

(8) Oltaya Gelme (Phishing) ..... 72

(9) Tarama (Scanning) ..... 72

(10) Bukalemun (Chamelon) ..... 73

(11) İstem Dışı Alınan Elektronik Postalar (Spam) ..... 73

(12) Çöpe Dalma / Atık Toplama (Scavenging).....	73
(13) Gizli Kapılar (Trap Doors) .....	73
(14) Sırtlama (PiggyBacking) .....	73
(15) Yerine Geçme (Masquerading).....	73
(16) Sistem Güvenliğinin Kırılıp İçeri Sızılması (Hacking) .....	74
(17) Hukuka Aykırı İçerik Sunulması .....	74
(18) Web Sayfası Hırsızlığı.....	74
(19) Sosyal Mühendislik .....	74
b. Siber Saldırı .....	74
c. Siber Terör .....	77
(1) Pasif Saldırıları .....	79
(2) Aktif Saldırıları.....	79
(3) Aktif ve Pasif Saldırıların Kullanımı .....	79
ç. Siber Savaş .....	83
3. Dünyadan Siber Terör Örnekleri .....	86
a. Çin Büyükelçiliğinin Bombalanması .....	87
b. Hainan Adası Olayı .....	87
c. Estonya .....	87
ç. ABD Gizli Askeri Ağında USB Olayı .....	88
d. Gürcistan .....	88
e. Conficker Solucanı .....	88
f. Cast Lead Harekâtı .....	89
g. Joint Strike Fighter – 35 (JSF-35) Verilerinin Çalınması.....	89
ğ. Mavi Marmara .....	89
h. Stuxnet.....	90
4. Siber Terörizme Karşı Siber Güvenlik Standartları .....	90
a. Bilgi Güvencesi .....	91
(1) Bilgi Güvencesi Temel Unsurları .....	92
(2) Bilgi Güvencesini Destekleyen Kavramlar .....	93

b. Temel Güvenlik Standartları..... 94

## **BEŞİNCİ BÖLÜM**

### **SİBER TERÖRİZMİN ETKİ ALANLARI..... 96**

1. Küreselleşme – Siber Terör ve Siber Tehdit İlişkisi ..... 96

2. Küreselleşme – Güvenlik ve Terör Örgütleri İlişkisi ..... 97

3. Terör Örgütleri – Sosyal Medya Kullanımı İlişkisi ..... 98

4. Terör Örgütleri – Asimetrik Siber Uzay Kullanımı İlişkisi..... 99

5. Geleneksel Terör ve Siber Terör Seçim Nedenleri ..... 100

6. Terör Örgütleri için Siber Terörizmin Çekici Unsurları..... 102

7. Siber Terörizmin Tehdit Potansiyeli ..... 102

8. Siber Terörizmin Türkiye Üzerine Etkileri ..... 104

9. Siber Güvenlik Konusunda Kurumlara ve Bireylere Düşen Görevler  
..... 105

### **SONUÇ ve ÖNERİLER ..... 108**

1. Sonuçlar ..... 108

2. Öneriler ..... 113

### **KAYNAKÇA ..... 118**

### **ÖZGEÇMİŞ..... 130**

## **KISALTMALAR**

ABD	Amerika Birleşik Devletleri
ARPANET	İleri Düzey Araştırma Proje Otorite Ağı (Advanced Research Projects Authority Net)
AR-GE	Araştırma Geliştirme
BITNET	Çünkü Ağ Zamanı (Because It's Time Network)
CCTA	(İngiltere) Merkezi Bilgisayar ve Telekomünikasyon Ajansı
CERN	Avrupa Araştırma Merkezi
COBIT	Control Objectives for Information and Related Technology
COMPUSEC	Computer Security – Bilgisayar Güvenliği
COMSEC	Communication Security – İletişim Güvenliği
Covid – 19	Korona Virüs
CSM	Sürekli Güvenlik İzleme Çatısı (Continuous Security Monitoring)
DARPA	Savunma İleri Düzey Araştırma Projeleri Kurumu (Defence Advanced Research Project Agency)
DNS	Alan Adı Sistemi (Domain Name Sistem)
EARN	Avrupa Akademik ve Araştırma Ağı (European Academic and Research Network)

HTTP	HyperText Transfer Protokolü
INFOSEC	Information Security – Bilgi Güvenliği
IoT	Nesnelerin İnterneti (Internet of Things)
IP	Internet Protocol
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
JSF	Joint Strike Fighter
MSB	Millî Savunma Bakanlığı
NATO	Kuzey Atlantik Antlaşması Örgütü
NSFNet	Ulusal Bilim Vakfı (National Science Foundation)
R.H.A.	Red Hackers Association
SSCB	Sovyet Sosyalist Cumhuriyetleri Birliği
TCP/IP	Geçiş Kontrol Protokolü/İnternet Protokolü (Transmission Control Protocol/Internet Protocol)
TCSEC	Trusted Computer System Evaluation Criteria
TSK	Türk Silahlı Kuvvetleri
TÜVEKA	Türkiye Üniversiteler ve Araştırma Kurumları Ağı
WWW	World Wide Web

## **TABLÖLAR**

	<u>Sayfa</u>
Tablo 1 Ülkelerin NATO'ya Üyelik Tarihleri	28
Tablo 2 Bazı Web Sitesi Olan Terör Örgütleri ve Yayın Yaptıkları Diller	56
Tablo 3 Geleneksel Saldırı ve Siber Saldırı Arasındaki Farklar	67
Tablo 4 Siber Eylemlerin Sınıflandırılması	68
Tablo 5 RedHack'in Yaptığı Saldırıları ve Olaylar	76
Tablo 6 Klasik Terör ile Siber Terör Arasındaki Farklar	78
Tablo 7 Siber Terör Eylem Düzeyleri	82
Tablo 8 Stuxnet Solucanından Etkilenen Ülkeler ve Etkilenme Yüzdeleri	90
Tablo 9 Yaygın Güvenlik Standartları	94

## ŞEKİLLER

	<u>Sayfa</u>
Şekil 1 Küreselleşme ve İşletmelerin Stratejik Ortaklık Oluşturma Nedenleri	19
Şekil 2 Toplam Küresel Stratejinin Elemanları	
Geçiş Aşamaları	23
Şekil 3 Terörizm, Siyasal İletişim Üçgenleri ve İnternet	40
Şekil 4 Terör Örgütlerinin Finansman Sağlama Süreci	60
Şekil 5 Soğuk Savaş Sonrası Güvenlik Kavramının Değişen Boyutu	65
Şekil 6 Bilgi Güvencesi Unsurları	92

## **RESİMLER**

	<u>Sayfa</u>
Resim 1 NATO Ana Teşkilatı	27
Resim 2 Colossus	33
Resim 3 İnternet	34
Resim 4 Servis Sağlayıcılarının Güvenli İnternet Hizmetleri	38
Resim 5 Terör Saldırısı Sonrası Görüntüler	44
Resim 6 Kolluk Güçleri Tarafından Ele Geçirilen Terör Malzemeleri	47
Resim 7 Terör Örgütleri İnternet Kullanımı	49
Resim 8 Terörist Ziyad Khaleel	62
Resim 9 ENIAC	69
Resim 10 Red Hackers Association (RedHack)'in Tanıtım Afişi	76





## GİRİŞ

### 1. Kitabın Amacı

Bu kitapta, on sekizinci yüzyılın ortalarından itibaren gelişen teknoloji ve yirminci yüzyılın son çeyreğinde önem kazanan küreselleşme nedeniyle sınırları yok olan devletlerin ve bu açıklardan faydalanmaya çalışan terör örgütlerinin siber uzay ortamında karşı karşıya geldiği siber terörizm kavramının incelenmesi amaçlanmıştır. Ayrıca siber uzayda meydana gelen diğer kavramlar olan siber suç, siber saldırı ve siber savaş kavramları da birbirlerinden ayırt edilebilmesi bağlamında incelemeye alınmıştır.

### 2. Kitabın Önemi

Özellikle 2. Dünya Savaşı ve akabinde sürdürülen Soğuk Savaş dönemi sonrasında sanayi toplumları bilgi toplumuna evrilmiş ve artan küreselleşme olgusu ile birlikte üreten ekonomilerde bilginin rolü giderek artmıştır. Artan bilgi, teknoloji gelişimine ve teknolojinin gelişimi de yeni bilgilerin açığa çıkmasına vesile olmuş, dolayısı ile toplumsal etkileşim ve dönüşümler geçmişe nazaran aşırı bir ivme kazanmıştır. Özellikle bilişim teknolojilerinde görülen hızlı gelişmeler toplumların etkileşimini arttırmış ve toplumlar üzerinde olumlu ve olumsuz yönde bir etki bırakmıştır. Bu bağlamda bilişim teknolojileri ulusal anlamda ekonomik, sosyal, politik ve kültürel alanlarda birçok değişime neden olurken, uluslararası anlamda terör ve terörizm kavramlarını küresel boyutlara taşımıştır.

Gelişen teknoloji paralelinde teknolojiye ulaşmanın kolaylaşması ve ucuzlaması sayesinde başta yeni kuşaklar olmak üzere toplumun tüm kesimleri sanal âlemlerde çok daha fazla vakit geçirmektedirler. Buna paralel olarak dijitalleşme kamu, özel kurum ve kuruluşlarda da yaygınlaşmaktadır. Bu bağlamda istihbarat ve istihbarata karşı koyma birimlerinin de bilişim teknolojilerinden yoğun olarak faydalandıkları şüphe götürmez bir gerçektir. Bilişim ve iletişim teknolojilerinde en iyiye ulaşmada rekabet içinde olan devletler ve/veya diğer örgütlenmeler de siber güvenlik ve siber savaş uygulamalarında ciddi değişimlere gitmektedirler. Bu değişimlerde, günümüz siber ordularının veya örgütlerinin bilişim teknolojilerindeki üstünlükleri göz önüne alınırken siber silah ve komuta-kontrol sistemlerinin güvensizlik ikilemi (security dilemma) olgusu önem kazanmaktadır. Bu bağlamda çalışmada, günümüzün ve geleceğin yeni savaş ortamı siber uzay kavramının terör örgütleri ve düşman devletler tarafından kötü amaçla kullanılması ve buna karşı önlemler alınmasının önemi vurgulanmaktadır.

## BİRİNCİ BÖLÜM

### KÜRESELLEŞME KAVRAMI

#### 1. Küreselleşme Öncesi Dünya Düzeni: Monarşiler ve Ulus Devletler

Orta Çağ Avrupası'nda kilisenin krallara taç giydiren siyasi ve başlılara dayalı ekonomik gücü ile asil kana sahip olduğu değerlendirilen toprak sahibi feodal beylerin egemenliğinden kurtulma süreci on ikinci yüzyılın ilk yıllarında başlamıştır. On beşinci yüzyıldan itibaren ise Karl Marx tarafından “*orta sınıf (Mittelstand)*”<sup>1</sup> olarak adlandırılan, soylu veya köylü sınıfına dâhil olmayan ve sosyal statüsünü eğitiminden, sahip olduğu üretim araçlarından, işveren konumundan ve ticari ilişkilere dayalı zenginliğinden alan liberal görüşlü burjuva sınıfı ortaya çıkmıştır. Feodal yapının iyice zayıflaması ile evlerini, barklarını kaybetmeye başlayan insanların ise ellerinde sadece emek gücü kalmıştır. Ne kadar çalışırsa çalışsın burjuva sınıfının boyunduruğundan kurtulamayan bu ücretli köle düzenini oluşturan işçi sınıfı insanları yine Karl Marx tarafından “*proletarya*”<sup>2</sup> olarak adlandırılmıştır. Emeğinin karşılığını alamayan proleterler ile onların üzerinden zenginliklerine zenginlik katan burjuvalar arasında çıkan sınıf mücadelesi ise toplum yapılarında değişikliğe gidilmesine zemin hazırlamıştır.

---

<sup>1</sup> Karl Marx ve Friedrich Engels, **Komünist Manifesto**, Çev.: Celal Üster ve Nur Deriş, Can Yayınları, E-Kitap 1. Baskı, İstanbul 2014, s.70.

<sup>2</sup> A.g.e. s.80.

Sanayi Devrimi ile birlikte gelişen teknoloji ve üretim sistemlerinin yanı sıra iletişim, ulaşım ve lojistik süreçleri de olumlu yönde etkilenmiştir. Buhar teknolojisi ile taşıma kapasitesi ve taşıma mesafesi artan ulaştırma araçlarının yaygınlaşması birbirinden çok uzak olan yerler arasında bile ticari etkileşimlere önyak olmuştur. Başlangıçta tarımsal ve endüstriyel ürünlerin ticareti olarak başlayan bu etkileşimler, çok farklı coğrafi noktalarda yaşayan insanları birbirlerinin yaşam tarzı, ekonomik güçleri, tarihsel süreçleri ve yönetim çeşitleri gibi birçok konuda karşılıklı bilgi sahibi yapmış ve çok önemli sonuçlara neden olmuştur<sup>3</sup>. Bu bağlamda Sanayi Devrimlerinin önemli siyasi, politik, ekonomik, sosyo-kültürel ve nihayetinde toplumsal dönüşümlere neden olduğu değerlendirilmektedir.

Milliyete dayalı birlik anlayışının ve ideolojinin güçlenmesi; sınır, egemenlik, bayrak kavramlarının kutsallaştırılması ulus-devlet anlayışını getirmiş ve orta işçi sınıfının da refah seviyesi yavaş yavaş artmıştır. Refah seviyesindeki bu artış işçi sınıfı da dâhil olmak üzere sermaye birikimine neden olmuştur. Sermaye birikimi ise daha fazla satış için daha fazla üretime ve dolayısı ile daha fazla hammadde isteğine neden olmuştur. Hammadde yarışındaki bu süreç kanlı sömürgecilik faaliyetlerine, pazar kavgalarına neden olarak milyonlarca hayatın kaybını da beraberinde getirmiştir.

Yirminci yüzyıl ile birlikte kas gücü yerine beyin; parasal sermaye yerine bilgi sermayesi değer kazanmaya başlamıştır. Bilgi değerinin

---

<sup>3</sup> Zekai Savaşlar, **Küreselleşme ve Sosyal Boyutu**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul 2007, s.3-4.

anlaşılması Sanayi Devrimi'nin temel teknoloji algısının değişmesini tetiklemiş ve yavaş yavaş sınırlar, paralar, bayraklar, konvansiyonel silah sistemlerine sahip ordular değerini yitirmiştir. Bu bağlamda ortaya zekâ ve bilgisi ile zenginlik üretebilen insan kavramı çıkmıştır.<sup>4</sup>

Yirminci yüzyılın ortalarında kendini gösteren ve yüzyılın sonlarından itibaren etkisini arttıran küreselleşme kavramı işletmecilik yaşamına çok büyük etkide bulunmuştur. Yirmi birinci yüzyıla gelindiğinde ise uluslararasılaşma ve çok ulusluluk yerine küresel çapta işlem hacmine sahip firmalar etkinliği ele almakta ve pazar rekabetinde yerel nitelikli rakiplerinden üstünlüklerini ortaya koymaktadırlar. Çünkü küresel işletmeler dünyanın en ücra köşelerinden temin ettikleri üretim kaynakları ile maliyeti düşürmekte, ürün standartlaştırmasını sağlamakta ve elde ettiği yüksek gelir ile Araştırma Geliştirmeye (Ar-Ge) yatırım yaparak üretim teknolojilerini geliştirip kaliteyi arttırmaktadırlar. Bu bağlamda karşımıza küresel ve uluslararası kavramları çıkmaktadır.

## **2. Uluslararasılaşma ve Küreselleşme**

İster Krallık olsun, isterse Ulus-Devlet, hiçbir ülke her şeyi kendi başına üretemez. Bunun en önemli nedeni üretilecek ürün için gerekli olan hammaddelerin tüm dünyada eşit bir şekilde dağılmamış olmasıdır. Bu nedenle ülkelerin coğrafi gücü temel alındığında tüm tarım ürünlerinin yetiştirilmesi, sanayi ve teknoloji ürünlerinin geliştirilmesine engel teşkil etmektedir. Gelişen teknoloji ile istenilen yerde, istenilen tarım ürünlerinin üretilebileceği düşünülse de

---

<sup>4</sup> Mehmet Altan, **Küresel Vicdan**, Timaş Yayınları, 1.Baskı, İstanbul, 2011, s.159

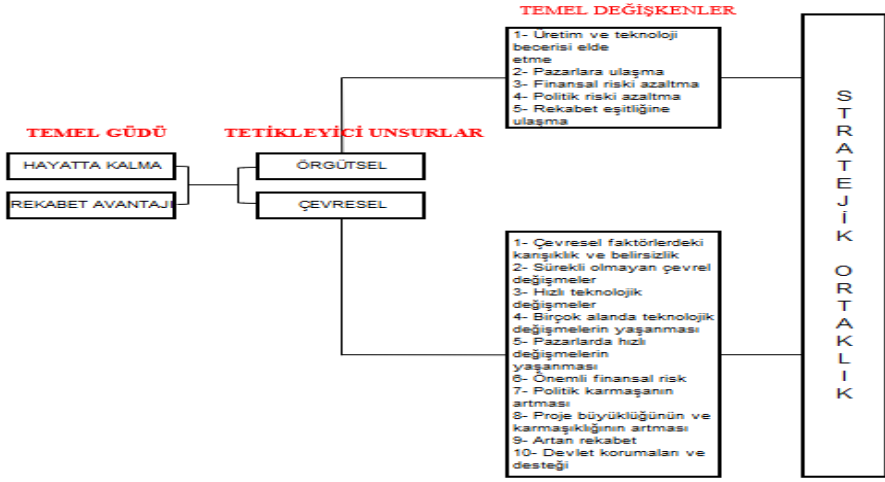
ülkelerin üretim maliyetleri yönünden bu yöntemi pek tercih etmedikleri değerlendirilmektedir. Dolayısı ile ülkeler ihtiyaçtan fazla üretilen ürünlerini satarak ihtiyaçları olan hammadde, ara madde ve son ürünleri almaktadırlar.

Üretim yönüne işletmeler açısından bakıldığında ise, işletmeler artan küreselleşme ve gelişen teknoloji sayesinde rekabet avantajlarını korumak, işletmenin var olmasının devamlılığını sağlamak, yeni gelişen veya başka bir ülkedeki endüstri kollarına girebilmek için sahip oldukları uzmanlıkları ve kaynakları birbirilerinin kullanımına vererek stratejik işbirliği oluşturmaktadır.<sup>5</sup> Çünkü bir ülkedeki işletmeler arasında var olan rekabet savaşı küreselleşmenin etkisiyle tüm dünyada artmakta ve bu nedenle stratejik iş birlikleri aynı faaliyet kolunda iş yapan tüm işletmeler arasındaki rekabette bir temel yapı taşı olmaktadır.<sup>6</sup> Bu bağlamda en alt basamakta üretim faaliyeti oluşturmaya çalışan örgütlerin de diğer örgütlerle ilişki kurmaya ihtiyaç duydukları ortadadır. Şekil 1’de gösterildiği üzere işletmeler hayatta kalmak ve rekabet avantajını sürdürebilmek güdüsü ile hareket etmekte ve bunu sağlayabilmek için çevresel ve örgütsel değişkenleri sağlamak için stratejik ortaklıklara girmektedir.

---

<sup>5</sup> Cemalettin Ö. Fidanboy ve Hale Alan, “Kaynak Bağımlılığı ve Stratejik İşbirliği İlişkisi:Kaynak Özelliklerinin İşbirliği Oluşumuna Etkileri”, **Savunma Bilimleri Dergisi**, Cilt: 12, Sayı:1, Mayıs 2013, s.127.

<sup>6</sup> Özlem Balaban ve Elvan Yıldırım Okutan, “Ekonomik Krizlerin Bir Sonucu Olarak Stratejik İşbirlikleri ve Şirket Birleşmelerinde Yönelim Uyum Değerlendirilmesine Yönelik Bir Araştırma”, **Journal of Azerbaijani Studies**, Cilt: 12, Sayı: 1, 2009, s.299-310



Şekil 1 – Küreselleşme ve İşletmelerin Stratejik Ortaklık Oluşturma Nedenleri<sup>7</sup>

Hayatta kalma ve rekabet avantajını sürdürebilme güdüsü ile hareket eden ve bu sayede üretim faaliyetini devamlı kılmaya çalışan örgütlerin de diğer örgütlerle ilişki kurmaya ihtiyaç duydukları ortadadır. Bu ilişkiler, zaman içerisinde farklı boyutları kapsayan kavramlara neden olmuştur. Bunlardan ikisi uluslararasılaşma ve küreselleşme kavramlarıdır.

Uluslararasılaşma, uluslararası ticari ilişkilerde bulunan kurum ve kuruluşları, uluslararası örgütleri ve çok uluslu şirketleri kapsamaktadır.<sup>8</sup> Bu bağlamda uluslararasılaşma, uluslararası ilişkileri, anlaşmaları, antlaşmaları, ortaklıkları ve ittifakları ifade etmektedir.<sup>9</sup> Uluslararasılaşma yöntemlerine bakıldığında işletmelerin kendileri ile

<sup>7</sup> Edwin A.Murray,Jr ve John F. Mahon, “Strategic Alliances:Gateway to the New Europe?”, **Long Range Planning**, Cilt: 26, Sayı: 4, 1993, s.104.

<sup>8</sup> Mustafa Delican, “Uluslararasılaşma ve Küreselleşme Bağlamında Karşılaştırmalı Endüstri İlişkileri: Gelişmeler ve Teorik Yaklaşımlar”, **Sosyal Siyaset Konferansları**, 2017/1/72, 20.02.2018, s.4-5.

<sup>9</sup> Altan,**a.g.e.**,s.101.



aynı sektörde; fakat farklı ülkede faaliyet gösteren işletmeler ile farklı türlerde ortaklıklar kurdukları görülmektedir. Bu ortaklık türleri:

### **a. Lisans Anlaşmaları**

Bir işletmenin başka bir ülkedeki işletmeye üretim lisansı vererek herhangi bir yatırım sermayesi ayırmadan faaliyet gösterme hakkını elde etmesidir. Lisansı alan işletme ise AR-GE çalışması ve ithalat yapmadan pazarda bilinen bir markayı üretip satma hakkını elde edebilir. Bu ortaklık türünün dezavantajı ise lisansı alan işletme lisansı aldığı işletmenin teknolojisini kullanmak durumunda kalırken, lisansı veren işletme kontrol kabiliyetini kaybetmektedir.

### **b. Franchising Anlaşmaları**

Bu ortaklık türünde de franchise veren işletme, franchise alan işletmenin bulunduğu ülke pazarına hiçbir yatırım yapmadan giriş hakkı elde etmektedir. İki firma birbirine sözleşme ile bağlanmaktadır. Nasıl yapılır (Know-How) ve markanın imtiyaz hakkının kullanıldığı bu anlaşma türünde sözleşme süre, sınırlar ve belirli şartları içermekte ve iki işletme arasında sürekli bir borç ilişkisi sağlamaktadır. Franchising girişimciler için sistem ve marka kullanımını içeren, know-how, lisans, taşeronluk ve bayilik gibi iş birliklerini kapsayan gelişmiş stratejik iş birliği türü olarak değerlendirilmektedir.

### **c. Ortak Girişimler**

Farklı iki ülkedeki iki ya da daha fazla işletmenin ortaklık yaparak diğer ülke pazarına giriş hakkı elde etmesidir. Bu ortaklık, genelde

büyük bir projede işletmelerin birbirlerinin güçlü yönlerinden istifade etmek amacıyla olur.

### **ç. Yeni İşletme Kurma veya Satın Alma**

Bir işletmenin yabancı bir ülke pazarına girmek için o ülkedeki bir işletmeyi satın almasıdır. Çünkü yeni işletme kurma işlemi oldukça riskli ve yüksek miktarda bir sermaye gerektirmektedir.

Uluslararasılaşma sürecinin zorluk yaratan durumları ise ülkeler arası zaman farkı, dil engelleri, farklı hukuk kuralları vb. şeklinde sıralanabilir. Ancak işletmeler için maliyetlerin, işçi giderlerinin azalmış olması yeterli olmaktadır.

Sonuç olarak uluslararası işletmecilik, ülke sınırlarını aşan ekonomik çalışmaların yaygınlaşmasını ve artmasını ifade etmektedir. Dolayısı ile uluslararasılaşmanın yeni bir olgu olmadığı ortadadır. Küreselleşme ise uluslararasılaşmanın çok daha ileri, karmaşık durumunu, yani bir işletmenin dünyanın çeşitli yerlerine yayılmasını ve bu dağılık ekonomik çalışmaların bir ölçüde entegrasyonunu ifade etmektedir. 1980 yılından itibaren sosyal bilimler literatürüne giren küreselleşme günümüzde ekonomik gelişmeleri ifade etmede kullanılmaktadır.<sup>10</sup>

Küreselleşme ticari ilişkileri ilgilendiren kavramların, aktörlerin, süreçlerin ve düzenlemelerin uluslararası düzenlemelerden bağımsız olarak yönetilmesidir.<sup>11</sup> Diğer bir ifade ile küreselleşme; dünyanın

<sup>10</sup> Erol Eren, **Stratejik Yönetim ve İşletme Politikası**, Beta Yayıncılık, 8. Baskı, İstanbul 2010, s338.

<sup>11</sup> Delican,**a.g.e.**, s.4-5

konumsal anlamda birbirine çok uzak iki egemen devletinde hem bireysel hem de toplumsal yaşamda, ekonomi, sosyo-kültürel, siyasi ve teknoloji alanlarında güçsüz egemen devletin güce hükmedenlerin isteği doğrultusunda değişimlere maruz kalmasıdır.<sup>12</sup> Bilgi ve iletişim teknolojilerindeki gelişim sayesinde küreselleşme süreci oldukça hızlanmış hatta yerel ve bölgesel sorunlar bile çok kısa sürede dünya çapında bir olguya dönüşmüştür.<sup>13</sup>

Küreselleşme kavramı sadece ekonomi alanında ele alınmamalıdır. Bu bağlamda sağlık sorunları, salgın, kirlilik, iklim değişikliği gibi kavramları kapsayan çevresel küreselleşmeden; nükleer tehdit, kutuplaşma, etnik, din ve mezhepsel ideoloji temelli terör örgütleri, asimetrik savaş gibi kavramları kapsayan askeri küreselleşmeden ve anayasal düzenin gelişmesi, demokratikleşmenin yaygınlaşması, kültür, göç ve dini fikirlerin yayılmasını kapsayan toplumsal küreselleşmeden de bahsedilebilmektedir.<sup>14</sup> Sonuç olarak insanlığa birçok olumlu etkisi olan küreselleşme olgusu, terörü de uluslararası boyuta taşıyarak terörün de küreselleşmesine neden olmaktadır.

Küreselleşmeyle birlikte, birçok insan etkinliği, giderek büyüyen bir dizi evrenselleştirilmiş kural ve standart ortaya çıkarmıştır. Egemen ulusal devlet ve toplum tarafından sağlanan eski koruyucu zırh zayıflamış ve bu bağlamda yerel faaliyet gösteren örgütler ve kurumlar küreselleşme ağıyla birbirine bağlantılı hale gelmiştir. Bu

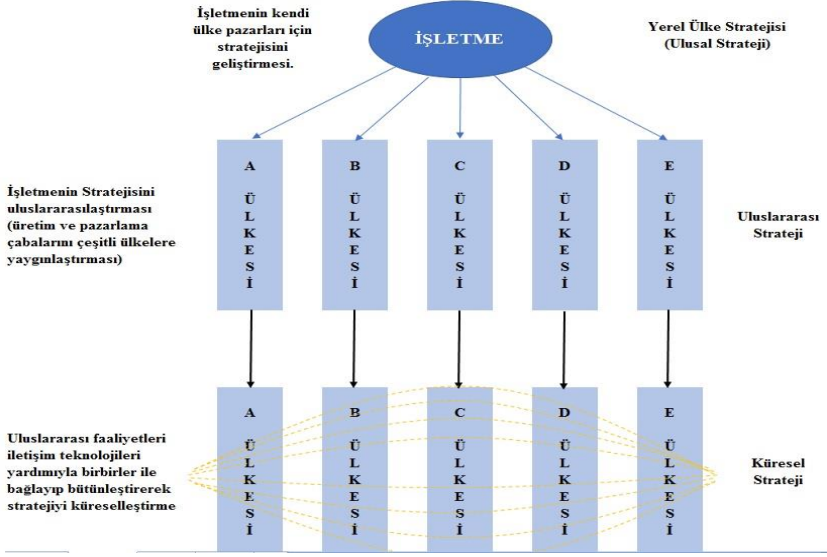
---

<sup>12</sup> Çetin Kartal, “Küreselleşme Sürecinin Devlet Yapısı Üzerine Etkileri”, **Ankara Barosu Dergisi**, 2016/2, 22.06.2016, s.290

<sup>13</sup> Hülya Baykal ve Tan Baykal, “Küreselleşen Dünya’da Çevre Sorunları”, **Mustafa Kemal Üniversitesi Sosyal Bilimler Dergisi**, 2008/5/9, 2008, s.2.

<sup>14</sup> Kartal, **a.g.e.**, s.294-314.

bağlantının kapsamı içinde bulunduğumuz küreselleşen çağa özgüdür. Bu noktada modern küreselleşmenin ekonomik değişimden ziyade siyaset, kültür ve kimlik gibi birçok sosyal varlığın organize aktörlere dönüşümünün merkezinde olduğu görülmektedir.



Şekil 2 – Toplam Küresel Stratejinin Elemanları ve Geçiş Aşamaları<sup>15</sup>

Şekil 2’de görüldüğü üzere bir işletmenin küresel strateji oluşturma isteği üç basamakta gerçekleşmektedir. Bunlar:

1. İşletmenin ana ülke pazarları için strateji üretmesi,
2. İşletmenin uluslararasılaşarak çeşitli ülkelerde üretim yapması ve pazarlama hizmetleri sunması,
3. İşletmenin uluslararası çalışmalarını birbiri ile bütünleştirerek küresel çapta stratejiler oluşturmasıdır. Bu bağlamda küresel

<sup>15</sup> Eren, a.g.e., s.341.

stratejinin oluşumunda başta iletişim olmak üzere teknoloji kullanımının payı oldukça büyüktür.

### **3. Teknolojik Gelişmenin Küreselleşmeye Etkisi**

Teknolojinin gelişmesi ile birlikte gerçek dünya yerini sanal dünyaya bırakmaktadır. Bu işlem o kadar hızlı olmaktadır ki güncel bir uygulamanın neredeyse bir yıl içinde eskidiği görülmektedir. Bunun yanı sıra kurumların kendilerini korumada kullandıkları güvenlik uygulamaları da gelişen siber terör uygulamaları karşısında savunmasız kalmaktadır. Dolayısı ile küreselleşmenin teknoloji uygulamaları üzerinde hem geliştirici hem de yıkıcı etkileri olduğu değerlendirilmektedir. Örneğin işletmelerin kullanmaya başladığı dijital kayıt sistemleri terör eylemleri sonucunda tüzel ve gerçek kişilerin gizli bilgilerinin açığa çıkmasına; işletmenin tuttuğu önemli kayıtları kaybetmesine neden olabilmektedir.

Endüstri 4.0 kavramı ile toplum hayatına giren akıllı ürünler kavramı gündelik hayatı kolaylaştırdığı kadar kişileri de terör eylemlerine de açık birer hedef haline getirmektedir. Örneğin casus yazılımlar (spyware) yardımı ile ortam dinlemesi ve görüntülenmesinden akıllı cihazdaki şifreli uygulamalara kadar giriş işlemleri yapılabilmektedir.

İçinde bulunduğumuz modern çağda herhangi bir örgütün genişlemesine ilişkin açıklamalar ister genel genişlemeye ister belirli örgüt türüne veya isterse de örgütsel bileşenlere odaklansınlar, küreselleşmeyi nedensel bir faktör olarak vurgulama eğitiminde

oldukları açıkça ortaya çıkmaktadır.<sup>16</sup> Bu tür açıklamaları önermek genellikle çok az teorik yaratıcılık gerektirir, çünkü örgüt yöneticileri örgütlerinin durumunu genellikle olduğunun üzerinde bir yerde yaparlar. Bu nedenle, geleneksel bir firmayı bir örgüte dönüştürmeyi öneren reformcular, rutin olarak küreselleşmeyi ve onun rekabetçi baskılarını gerekçe olarak önermektedirler. Buna ek olarak yoğunlaştırılmış mübadele ve rekabete yapılan bu vurgu, çeşitli küreselleşme anlayışlarında ortaktır. Sosyal bilimciler rutin olarak ulus-devlete, çok uluslu şirkete veya hükümet dışı birliğe başvurmakta ve küreselleşmeyi, bu birimlerin aralarındaki mübadele ve rekabetin yoğunlaşması olarak tanımlamaktadırlar.

Yoğunlaştırılmış mübadele ve rekabet olarak küreselleşme kavramları çoğunlukla ekonomik, bazen de askeri olarak tanımlanmaktadır. Çünkü örgütsel yapının genişlemesi rekabetçi baskıların işlevsel olarak arttığı anlamına gelmektedir. Bunun anlamı, daha yüksek düzeyde örgütlemiş birimlerin, çeşitli işlevsel sorunlar ortaya çıkaran, çağa uyma tutkusuyla hızla modernleşen rekabetçi bir bağlamdan gelen taleplere yanıt olarak çoğalmasındır. Buna göre uluslararası kuruluşlar yararlı olmasa da somut ve istikrarlı bir organizasyon yapısı için destekleyici bir idari aygıt aracılığıyla kolektif faaliyetlerin merkezileştirilmesine izin vermektedirler. Bu izinler kolektif faaliyetlerin verimliliğini artırmakta ve örgüt ve devletlere anlayışlarını, ortamını ve çıkarlarını etkileme becerisini geliştirme imkânı sunmakta dolayısı ile askeri faaliyetleri de etkilemektedir.

---

<sup>16</sup> Gili S. Drori vd., **Globalization and Organization**, Oxford University Press, 1. Baskı, New York 2006, s.7.

#### 4. Küreselleşmenin Askeri Yönü

İkinci Dünya Savaşı sürecinde ülkelerin teknoloji rekabeti üst düzeye çıkmış ve bilgiye ulaşma rekabeti başlamıştır. Soğuk Savaş Dönemi ile ipler biraz daha gerilse de sonrasında silahsızlanma ve güvenlik işlemlerinde atılan adımlar sayesinde kısa süreli çatışmalar önemli ölçüde anlaşmalar ile sonuçlanmıştır.<sup>17</sup>Buna ek olarak yapılan askeri eğitimler ve tatbikatlar askerlerin de küresel boyutta birbirlerinden etkilenmelerine neden olmuştur. Ancak ülkeler arasındaki bu kolektif birliktelikler zamanla ülkelerin kendi güvenliklerini sağlama konusunda tek başlarına belirleyici rol üstlenmelerini imkânsız hale getirmiştir. Çünkü küreselleşme ile ülkelerin birbirlerine olan bağımlılıkları artmıştır. Bu bağlamda, artan bağımlılık ülkelerin maddi ve askeri güçlerini kullanacakları zaman siyasi, ekonomik, toplumsal ve çevresel değişkenleri de hesaba katmaya dolayısı ile küresel ittifaklar kurmaya zorlamaktadır.<sup>18</sup>

Küreselleşme askeri yönden ele alındığında en önemli örgütün NATO (Kuzey Atlantik Anlaşması Örgütü-The North Atlantic Treaty Organization) olduğu değerlendirilmektedir. Siyasal açıdan Sovyet Sosyalist Cumhuriyetleri Birliği'ne (SSCB) karşı kurulan NATO'nun temel misyonu üye ülkelerin özgürlük ve güvenliklerini sağlamaktır. Bu bağlamda küresel tehditlere karşı hali hazırda kurulmuş küresel bir güvenlik örgütü bulunmaktadır. Bu bağlamda Resim 1'de NATO'nun

---

<sup>17</sup> Devlet Planlama Teşkilatı, **Küreselleşme ve Özel İhtisas Raporu**, DPT yayını, Ankara 2000, s.51

<sup>18</sup> Mehmet Aktel ve Muharrem Gürkaynak, "Küreselleşen Terörizm: Bir Etkileşim Çalışması", **38. ICANAS (Uluslararası Asya ve Kuzey Afrika Çalışmaları Kongresi)**, Sayı: 1, Cilt: 1, 2011, Ankara,s.77-88.

Ana Teşkilat Yapısı, Tablo 1’de ise üye devletler gösterilmektedir. Tablo 1’de ulusal güvenliklerini garanti almaya çalışan ülkelerin küresel güvenlik örgütlerine halen girmeye devam ettikleri görülmektedir.



Resim 1 – NATO Ana Teşkilatı<sup>19</sup>

<sup>19</sup> <https://www.nato.int/nato-welcome/index.html>, (Erişim Tarihi: 30.10.2020).



<u>Ülke</u>	<u>Üyelik Tarihi</u>	<u>Ülke</u>	<u>Üyelik Tarihi</u>	<u>Ülke</u>	<u>Üyelik Tarihi</u>
ABD	4 Nisan 1949	Portekiz	4 Nisan 1949	Estonya	29 Mart 2004
Belçika	4 Nisan 1949	İngiltere	4 Nisan 1949	Letonya	29 Mart 2004
Kanada	4 Nisan 1949	Türkiye	18 Şubat 1952	Litvanya	29 Mart 2004
Danimarka	4 Nisan 1949	Yunanistan	18 Şubat 1952	Romanya	29 Mart 2004
Fransa	4 Nisan 1949	Almanya	9 Mayıs 1955	Slovakya	29 Mart 2004
İzlanda	4 Nisan 1949	İspanya	30 Mayıs 1982	Slovenya	29 Mart 2004
İtalya	4 Nisan 1949	Çekya	12 Mart 1999	Arnavutluk	1 Nisan 2009
Lüksemburg	4 Nisan 1949	Macaristan	12 Mart 1999	Hırvatistan	1 Nisan 2009
Hollanda	4 Nisan 1949	Polonya	12 Mart 1999	Karadağ	5 Haziran 2017
Norveç	4 Nisan 1949	Bulgaristan	29 Mart 2004	K.Makedonya	27 Mart 2020

**Tablo 1 – Ülkelerin NATO'ya Üyelik Tarihleri<sup>20</sup>**

## 5. Küreselleşmenin İktisadi Yönü

Yirminci yüzyılın ikinci yarısından bugüne küreselleşmenin iktisadi yönünün temelinde kapitalizm yer almaktadır. Bu süreçte gelişme sürecini tamamlamış ülkeler tüm mevduatların altın ve dolara endekslemişler ve bu bağlamda küresel kapitalizmin yerleşmesine önemli katkıda bulunmuşlardır. Buna ek olarak bölgesel işletme ve örgütlerde ticari sınırlılıkların kaldırılması için çabalamış, ürün ve hizmetlerin sıkıntısız bir şekilde akışının sürdürülebilmesi için bütünleşme sürecini hızlandırmışlardır. Özellikle 1989 yılında

<sup>20</sup>[https://www.nato.int/cps/en/natohq/topics\\_52044.htm](https://www.nato.int/cps/en/natohq/topics_52044.htm), (Erişim Tarihi: 26.12.2020.)

komünist SSCB'nin dağılması ile bağımsızlığına kavuşan ülkeler serbest piyasa ekonomini benimsemiş ve kapitalizm bütünleşmesi tamamen küreselleşmiştir.

Kapitalizme yöneltilen en büyük eleştirilerden biri gelir dağılımının dengesizliğidir. Bu dengesizlik beraberinde eğitim eşitsizliğini getirmektedir. Dünya nüfusunun büyük bir kısmının gelir ve eğitim durumlarının düşük olması cahil halkın kandırılmasında, bir parça zenginlik için her türlü faaliyete katılmasına neden olmaktadır. Bu faaliyetlerden biri de terör eylemidir.

## **6. Küreselleşmenin Sosyal Yönü**

Kültür, toplumların temel değerlerini, davranış biçimlerini ifade etmektedir. Kültür, toplumdan topluma değişiklik gösterdiği gibi zamansal yönden aynı bölgede yaşamış toplumlarda bile değişiklikler göstermektedir. Bununla birlikte aslında toplumlar yavaş bir hızla da olsa diğer toplumlar ile kültürel etkileşim içinde bulunmuşlardır. Ancak modern çağın bilişim teknolojisi sayesinde bu etkileşim aşırı derecede hızlanmıştır. Bu hızlanma ise dünya genelinde tüm toplumları içine alacak benzeşmelerle kültürel küreselleşmeyi beraberinde getirmiştir.

Kültürel küreselleşmenin oluşmasının temel yapı taşlarından biri İngilizcedir. Dolayısı ile İngilizcenin yanı sıra teknolojik gelişimi ve ekonomisi ile kültürel küreselleşmede Amerika Birleşik Devletleri (ABD) ağırlığı hissedilmektedir. Bunun en büyük göstergesi McDonald's, Starbucks, Youtube, Netflix gibi popüler kültürün küresel firmalarının ABD merkezli olmasıdır. Bu firmaların en çarpıcı

örneği Netflix'tir. Bu firma yerel senaryolarla ülkede yeni teknoloji ile film ve dizi üretimine olanak sağlamaktadır. Bu bağlamda, eğer istenirse, kötü niyetli kişi veya örgütlerin film ve dizilerde propaganda yapma ve bu propagandayı dünyaya duyurma olanağına kavuştuğu değerlendirilmektedir.

## 7. İletişim Araçlarının Küreselleşmeye Etkisi

1991 yılı sonrasında yavaş yavaş sivilleşen ve tüm toplumların kullanımına sunulan internet, birey, toplum ve devletleri birbirlerine daha etkin şekilde bağlamış ve hali hazırda bu özelliğini devam ettirmektedir. Bu bağlamda, internetin küresel olayların oluşumu hızlandıran bir etmen olduğunu söylemek oldukça gerçekçi bir bakış açısı sunmaktadır. İnternet, tüm insanlığın zihnindeki Soğuk Savaş korkusunun azalmasında ve farklı taraflardaki insanlar arasındaki farklılıkların azalarak ortak yönlerin oluşmasında önemli bir rol oynamıştır.<sup>21</sup>1991 Körfez Savaşı gidişatının internet ve medya üzerinden anlık olarak izlenmesi gelecekteki dünyanın bambaşka bir hal alacağına en büyük göstergesi olmuştur. Bu nedenle, Körfez Savaşı “iletişim savaşı” olarak lanse edilmiştir.<sup>22</sup>

Küreselleşme sürecini hızlandıran etkenlerin en önemlisi iletişim alanında yaşanan gelişmelerdir. Radyo, televizyon, telefon gibi ürünlerin özellikleri aynı cihazda sunulmaya başlanmış olmakla beraber gün geçtikçe daha da bireysel hale gelmektedir.

---

<sup>21</sup> Salih Bıçakçı, “Yeni Savaş ve Siber Güvenlik Arasında NATO’nun Yeniden Doğuşu”, **Uluslararası İlişkiler**, Cilt 9, Sayı 34, Yaz 2012, s.207.

<sup>22</sup> Armand Mattelart, **Mapping World Communication: War, Progress, Culture**’, Minneapolis, University of Minnesota, Minnesota 1994, s.117.

İletişim alanındaki ilerlemenin en iyi göstergesi internettir. İnsanları birbirine bağladığı, uzakları yakın ettiği şeklinde övgülere mazhar olan internet ticaretten endüstriye, basın ve yayın organlarından kütüphanelere, evlerden iş yerlerine ve daha birçok alanı birbiri ile bağlamaktadır.

Soğuk Savaş'ın son bulması ve küreselleşmenin etkisiyle dünya düzeninin değişmesi ve savaş kavramının tanımından aktörlerine; amaçlarından taktik ve stratejilerine ciddi bir dönüşüm ve farklılaşma yaşadığı gözlemlenmiştir. Bu doğrultuda yeni konjonktürü Herfried Münkler ve Marry Kaldor “yeni savaşlar” olarak, Lind ise “dördüncü nesil savaşlar şeklinde tanımlamışlardır.<sup>23</sup> Çünkü geleneksel tanımlamalar artık yeni durumları açıklamakta yetersiz kalmıştır. Kaldor’a göre yeni savaş tanımında, küreselleşmenin yaygınlaşması ile birlikte değişim gösteren sosyo-politik, ekonomik ve kurumsal çerçeveler ulus devlet sistemlerini ve sert milli güç unsuru olarak gösterilen askeri güç kullanımını değiştirmiştir.<sup>24</sup> Bu güç değişimi bireysel suç faaliyetlerini, suç örgütlerini, terör gruplarını ve çeteleri yeni savaş ortamının yeni aktörleri haline getirmiştir.

---

<sup>23</sup> Sami Eker, “Savaş Olgusunun Dönüşümü: Yeni Savaşlar ve Suriye Krizi Örneği” **Türkiye Ortadoğu Çalışmaları Dergisi**, Cilt: 2, Sayı: 1, 2015, s.33.

<sup>24</sup> Mary Kaldor, **News and Old Wars**, Stanford University Press, 2.Baskı, California, 2007.

## İKİNCİ BÖLÜM

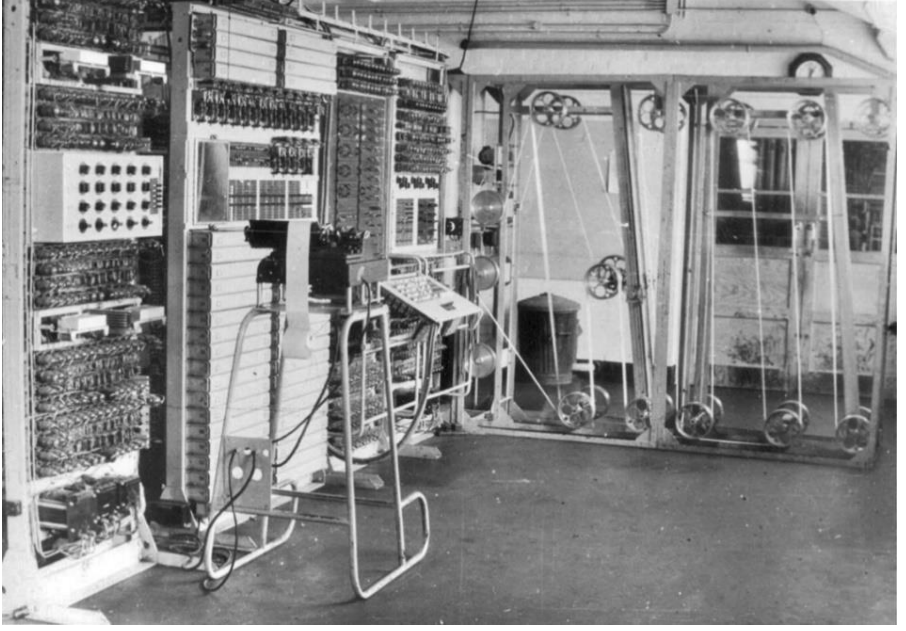
### TOPLUM İLETİŞİMİNDE YENİ BİR ARAÇ: İNTERNET

#### 1. İnternet Nedir?

İnternetin tarihi, aslında kitlesel telekomünikasyon tarihinin bir bileşenidir. Bu bileşen, 1837'de Samuel Morse'un telgraf vericisi ve alıcısını icat etmesiyle başlamıştır. Atlantik ötesi bir iletişim kablosu aracılığı ile yapılan beş denemeden sonra, 1866'da ulusal devletlerarasında coğrafi mesafeleri gerçek anlamda azaltacak ve neredeyse anlık iletişimin yolunu açacak temeller atılmıştır. İkinci dünya savaşı sırasında, bir anlamda Morse'un icadından yüz yıldan fazla bir süre sonra, Resim 2'de gösterilen 'Colossus'<sup>25</sup> (küçük bir ofis büyüklüğünde) olarak bilinen ilk yarı programlanabilir bilgisayar, Birleşik Krallık'ta Bletchley Park'ta kod kırma faaliyetleri için yapılmıştır.

---

<sup>25</sup> Colossus bilgisayarı, İkinci Dünya Savaşı sırasında yapılan şifreli Alman yazışmalarını çözmek için kullanılan erken dönem bilgisayarlardan biridir. Dünyanın ilk kısmen programlanabilen dijital elektronik bilgisayarıdır. <http://www.rutherfordjournal.org/article030109.html> (Erişim Tarihi 23.12.2020).



**Resim 2 – Colossus<sup>26</sup>**

İnternet, ister aynı ülkede isterse farklı ülkelerde olsun birçok bilgisayar veya akıllı cihaz sistemlerini TCP/IP<sup>27</sup> protokolü ile birbirine bağlayan ve küreselleşen dünya düzeninde sürekli olarak genişleyen kolay, ucuz ve hızlı bir iletişim ağıdır. İnternet adı ise İngilizce INTERNational ve NETwork kelimelerinin bir araya gelmesiyle oluşturulmuş olup Resim 3’de gösterildiği üzere birbirine bağlı bilgisayarlar ağı anlamında kullanılmaktadır. Bu bağlamda

<sup>26</sup> [www.telegraph.co.uk](http://www.telegraph.co.uk)

<sup>27</sup> TCP/IP (Transmission Control Protocol/Internet Protocol): Bilgisayar ile veri iletme/alma birimleri arasında organizasyonu sağlaya, böylece bir yerden diğerine veri iletişimini olanaklı kılanpek çok veri iletişim protokolüne verilen genel addır. TCP kısmı veri transferinde önemli noktaları belirtirken IP kısmı taşıma yolunu bulmayı belirtir.

İnternet kelimesinin ilk harfi birden fazla ağı birleştiren bağlantıları tanımladığı için her zaman büyük yazılmalıdır.



**Resim 3 – İnternet**

İnternetin tarihine bakıldığında ilk çalışmaların (paket anahtarlamalı ağ) 1960'ların sonunda Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı'na bağlı DARPA (Defence Advanced Research Project Agency)'ya ait ARPANET (Advanced Research Projects Authority Net)'in kurulması ile ortaya çıktığı ve TCP/IP protokolünün ise 1983 yılından itibaren ARPANET üzerinden kullanılmaya başlandığı görülmektedir.<sup>28</sup> Bu bağlamda ilk internet uygulama çalışmalarının askeri kullanım amaçlı olduğu açıktır. Buna ek olarak paket anahtarlamalı ağ yapısının düşmanın erişimini zorlaştırmak için kurulmuş ve erişimi hiyerarşiye göre belirlemekte olan ağ yapısı olduğu değerlendirildiğinde güvenlik çalışmalarının da yapıldığı değerlendirilmektedir. Bu süreci takiben öncelikle 1986 yılında

<sup>28</sup> Ahmet Parlak, **İnternet ve Türkiye'de İnternetin Gelişimi**, Fırat Üniversitesi Mühendislik Fakültesi, Bitirme Ödevi, Elazığ 2005, s.26.

NSFNet (National Science Founfation) tarafından ilk ağ oluşturulmuş olup 1989 yılından itibaren internet halka açık bir platform haline gelmiştir. İnternetin ticari amaçla kullanımı ise 1991 yılından itibaren ABD, Avrupa, Japonya ve diğer Pasifik ülkelerinde görülmüştür. Türkiye de ise ilk internet ağı 1986 yılında kurulan EARN (European Academic and Research Network) /BITNET (Because It's Time Network) bağlantılı TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) olduğu bilinmektedir. Türkiye, internete Orta Doğu Teknik Üniversitesi bünyesindeki TR-NET adlı kuruluş tarafından kiralan “.tr” uzantısı ile 12 Nisan 1993 tarihinden itibaren bağlıdır.<sup>29</sup>Günümüzde Küresel nüfusun yaklaşık %59'u internet kullanmaktadır.<sup>30</sup>

## 2. İnternette Erişim Nasıl Olur?

Geçmişte İnternet kullanıcılarının çoğu internete evlerinden, iş yerlerinden, üniversite veya ticari bir kuruluştan girerken, gelişen teknolojinin ve küreselleşmenin getirdiği olanaklar sayesinde artık internet günlük yaşantı ile iç içe geçmiştir. Hatta akıllı cihazlar ile bireysel manada internete erişmenin yanı sıra wifi özelliği bulunan tüm akıllı cihazların kullanıcıdan bağımsız bir şekilde internete eriştiği bir dünya düzeni yaşanmaktadır.

1989'da İsviçre'de bulunan CERN (Avrupa Araştırma Merkezi) “nde çalışan bir araştırmacının HyperText Transfer Protokolü (HTTP)”nü

<sup>29</sup> Ankara Barosu Bilişim Programı Sertifika Programı Notları, 2007.

<sup>30</sup> <https://www.sabah.com.tr/teknokulis/haberler/2020/02/24/dunyada-ne-kadar-insan-internet-kullaniyor> (Erişim Tarihi 29.09.2020).



ve URL'leri geliřtirmesi ile bugünkü anlamdaki World Wide Web (www) ortaya çıkmıřtır.<sup>31</sup>

Net üzerindeki her bir araç internet üzerinde iletiřim kurabilmek için IP (Internet Protocol) adresi olarak adlandırılan kendi özel kimlik numarasına sahip olmalıdır. Bu adres insanların kolay bir řekilde anlayabilmesi için noktalarla ayrılmıř ondalık sayılardan oluřmuř řekilde gösterilmektedir. Ancak bilgisayarlar ikili düzen (Binary) formatında iliřki kurdukları için IP adresleri farklılařmaktadır. Bu bağlamda bağlanmak istediđimiz yerlerin IP adreslerini yazmamız yeterlidir. IP adreslerinin ise her ne kadar noktalarla ayrılmıř ondalık sayı biçiminde gösterilse de akılda tutmak zordur. Bunun için IP adreslerinin isimlerini metin olarak adresleyen DNS (Domain Name System) sistemi oluřturulmuřtur. Bۆylelikle IP adresi yerine eriřmek istediđimiz metni yazmamız yeterli olacaktır.

### 3. İnternet Güvenliđi

Türk Dil Kurumu güncel sözlüđüne göre güvenlik terimi “*Toplum yařamında yasal düzenin aksamadan yürütölmesi, kiřilerin korkusuzca yařayabilmesi durumu, emniyet*”<sup>32</sup> anlamında kullanılmaktadır. Uluslararası iliřkiler perspektifinden bakıldığında ise bařta Arnold Wolfers olmak üzere güvenlik ile ilgili birçok arařtırmacı güvenliđin sahip olunan deđerlere yönelik herhangi bir

---

<sup>31</sup> Malik Aslanyürek, **İnternet Güvenliđi ve Çevrimiçi Gizlilik Alanlarında Yařanan Sorunlar: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliđi ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları Üzerine Bir Arařtırma**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara 2015, s.20-21.

<sup>32</sup> <https://sozluk.gov.tr> (Eriřim Tarihi 29.09.2020).

tehdidin olmaması olarak tanımlamaktadır.<sup>33</sup> Bu bağlamda güvenlik kavramına göre fiziksel boyutun ön plana çıkartıldığı görülmektedir. Ancak daha geniş açıdan bakıldığında güvenliğin fiziksel boyutunun yanı sıra, sosyal, toplumsal ve güç boyutlarının da olduğu görülmektedir. Güvenliğin güç boyutu kurumları ve özellikle devletleri ilgilendiren bir boyuttur. Dolayısı ile güvenlik kavramının güç boyutu devletin bekası ile ilgilidir. Bu yüzden devletler tarih boyunca güvenliklerini sağlamak için olağanüstü önlemler almış, gerektiğinde güç kullanmış ve bunu devletin korunması gerekçesine dayandırarak haklı olduklarını öne sürmüşlerdir.

Günümüzde güvenlik kavramı bambaşka boyutlar kazanmıştır. Bunlardan bir tanesi de gündelik hayatımızın vazgeçilmezi internettir. Özellikle çocuk kullanıcılara karşı işlenen suçlarla ve cinsel istismarlara karşı devletler tarafından gerekli önlemler alınarak yasal düzenlemeler yapılmaktadır. Bu bağlamda Avrupa Birliği Komisyonu, 1990'lı yılların sonundan itibaren “*Güvenli İnternet Programı*” düzenlemesini uygulamaya koymuştur.<sup>34</sup> Bu bağlamda Resim 3’de gösterildiği üzere tüm internet sağlayıcıları çocuk güvenliği ve aile güvenliği hizmetleri sunmaktadır.

---

<sup>33</sup> Murat Yorulmaz, “Değişen” Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde “Değişmeyen” Güvenlik Paradoksu, **Balkan Araştırma Enstitüsü Dergisi**,2014/3/1, 2014,s.107-108.

<sup>34</sup> Şahin Bayzan ve Alper Özbilen, “Dünyada İnternetin Güvenli Kullanımına Yönelik Uygulama Örnekleri ve Türkiye’de Bilinçlendirme Faaliyetlerinin İncelenmesi ve Türkiye İçin Öneriler”, **5. International Computer & Instructional Technologies Symposium (20-22 Eylül 2011, Elazığ) Bildiriler Kitabı**, Fırat Üniversitesi, Elazığ 2011, s.257-259.

İşletmecisi	Çağrı Merkezi	Online İşlem Merkezi	Çocuk Profili için	Aile Profili için
TURKCELL	444 0 532	turkcell.com.tr	GUVENLI COCUK -> 2200 *	GUVENLI AILE -> 2200 *
SUPERONLINE	0 850 222 0222	superonline.net	GUVENLI COCUK -> 2220	GUVENLI AILE -> 2220 *
AVEA	444 1 444	avea.com.tr	GUVENLI COCUK -> 5555	GUVENLI AILE -> 5555 **
TTNET	444 1 444	ttnet.com.tr	GUVENLI COCUK -> 6606	GUVENLI AILE -> 6606 **
VODAFONE	444 0 542	vodafone.com.tr	GUVENLI COCUK -> 7005	GUVENLI AILE -> 7005 **
VODAFONE NET	0 850 542 0 542	vodafone.com.tr	-	-
TURKISAT	0 850 804 44 44	turksat.com.tr	GUVENLI COCUK HIZMETNO -> 5126	GUVENLI AILE HIZMETNO -> 5126
DSMART	0 850 266 0266	dsmart.com.tr	GUVENLI COCUK ABRONENO -> 2850	GUVENLI AILE ABRONENO -> 2850 **
MILLENICOM	0 850 333 0333	milleni.com.tr	MILLENICOM COCUK -> 4730	MILLENICOM AILE -> 4730
TURKNET	0 850 288 8080	turknet.net.tr	GUVENLI COCUK -> 3371	GUVENLI AILE -> 3371 **
ESER TELEKOM	0 312 890 0 444	esertelem.com.tr	-	-
ISNET	-	isnet.net.tr	-	-
EXTRANET	0 850 470 0 444	extranet.com.tr	-	-



Resim 4 – Servis Sağlayıcılarının Güvenli İnternet Hizmetleri<sup>35</sup>

İnternet kullanımının yaygınlaşması ile birlikte bireysel çerçevede kültürel, zamansal ve toplumsal değerlere göre değişkenlik gösteren mahremiyet kavramı öne çıkmaktadır. Kısaca gizli kalması gereken şey anlamına gelen mahremiyet, Alan West tarafından “*Bireylerin, grupların ya da kurumların sahip oldukları bilginin ne zaman ve ne ölçüde diğerlerine aktarılabilceğini kendilerinin belirleme hakkıdır*” şeklinde tanımlanmıştır.<sup>36</sup>Bu bağlamda mahremiyet özerkliktir ve kişi veya kurumların sırlarını gizleme ve istediği ile paylaşma hakkını kapsamaktadır.

İnternet kullanımı hem güvenlik hem de mahremiyet kavramlarının en çok irdelendiği alanlardan biridir. Örneğin internet üzerinden bir ürün aldığımızda kart bilgilerinizin ve kişisel verilerinizin çalınması güvenlik açısından ve sipariş verdiğiniz ürünün açığa çıkarılması mahremiyeti açısından risk oluşturmaktadır. Buna ek olarak özel

<sup>35</sup> www.shiftdelete.net

<sup>36</sup> Malik Aslanyürek, a.g.e., s.14.

hayatın gizliliğini ihlal eden, sosyal ağlara kötü amaçlı yazılımlar ve virüsler gönderen kişi veya kişilerin de varlığı internetin diğer büyük riskleridir. Devlet tarafından oluşturulan güvenlik ekipleri ve güvenlik uygulamaları internet ortamında riskleri azaltmada toplum güvenliği için insanlar lehine önlemler almaktadır. Ancak bazı devletlerde iktidar sahipleri toplum güvenliğini sağlama amacından çıkıp internet ortamını, kişileri özellikleri muhalifleri gözetlemek için kullanmaktadır. Dolayısı ile toplum güvenliğini sağlamakla görevli olan devlet, elindeki büyük güçler sayesinde insanlar için tehdidin bizzat kendisi olmaktadır.

#### **4. Terör Bağlamında Medya ve Sosyal Medya**

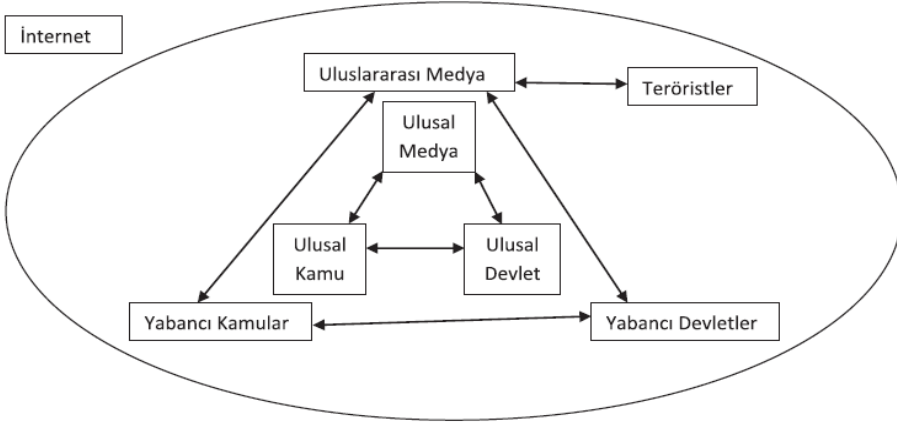
Günümüzün en çok kullanılan kavramların başında hiç şüphesiz medya kavramı gelmektedir. Gazete, dergi, radyo, televizyon ve tabii ki internet gibi kitle iletişim araçlarının tamamını içine alan medya kavramı tüm insanların en tabii hakkı olan haber alma hakkını kullanabilmesini sağlamaktadır.<sup>37</sup> İnsanlar haber alma haklarını kullanırken, medya sahipleri ve çalışanları ise hayatlarını kazanabilmek için gelir sağlamak ve aynı zamanda habercilik yapmak durumundadırlar. Bu da medya kurum ve kuruluşlarının maddi kaynak bulmak yükümlülüğünde bırakmaktadır. Bu bağlamda medya kurum ve kuruluşları yayınladığı yayınların ve programları izlenmesine; gazete ve dergilerin satılmasına hayati derecede ihtiyacı olmaktadır. Ancak her ne kadar gelire ihtiyaçları olsa da medya kurum ve

---

<sup>37</sup> Atahan Birol Kartal, “Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye’de DEAŞ ve YPG Örneği”, **Güvenlik Stratejileri Dergisi**, 2014/27, 16.04.2018, s.58-59.

kuruluşları, haber değeri olan yayınları yaparken devletlerin yürütmeye koyduğu yasaları uygulamakla yükümlüdürler. Buna ek olarak diğer bir husus ise medya kurum ve kuruluşları bilinçli veya bilinçsiz olarak terör örgütü gibi oluşumların propagandasını yapmaktan kaçınmalıdır. Çünkü medya kurum ve kuruluşları haber alma fırsatı kovalarken, terör örgütleri de toplumu etkilemek, korkutmak, yanlış yönlendirmek, meşruiyet kazanmak gibi amaçlarla yaptığı video ve haberleri medyaya servis etmektedirler.

Terör örgütleri küreselleşen dünyada istediklerini her zaman katı güç (hard power) ile çözülemeyeceğinin farkına vardıkları için yumuşak güç (soft power) olarak gördükleri medyaya dolayısı ile internete yönelmektedirler.<sup>38</sup>



Şekil 3 – Terörizm, Siyasal İletişim Üçgenleri ve İnternet<sup>39</sup>

<sup>38</sup> Zakir Avşar, İnternet Çağında Medya, Terör ve Güvenlik, **TRT Akademi**, 2017/02/03, 19.12.2016, s.112.

<sup>39</sup> Brigitte Nacos, Terrorism/Counterterrorism and Media in the Age of Global Communication, **United Nations University Global Seminar Second Shimame-Yamaguchi Session Terrorism – A Global Challenge**, 5-8 August 2006, s.4.

Medya organlarının toplumu bilgilendirmek, gerçekleri sunmak gibi yükümlülükleri varken devletlerde ulusal güvenliğini ve uluslararası saygınlığını koruma yönünde hareket etmektedirler. Şekil 2’de de görüldüğü üzere internet içerisinde Ulusal Medya Ulusal Kamu ve Ulusal Devlet arasında birbirini çevreleyen üçgenin dışında Uluslararası Medya Yabancı Kamu ve Yabancı Devletler üçgeni yer almaktadır. Bu bağlamda yabancı devletlerin uluslararası medyayı kullanarak ulus devletler üzerinde belirleyici bir rol oynamaktadır. İnternet ise dünyayı çevreleyen bilgi ağı sayesinde haber niteliği taşıyan veya taşımayan her türlü verinin dünyaya yayılmasına neden olmaktadır. Bu bağlamda terör örgütleri uluslararası platformda birbirleriyle, diğer terör örgütleri ile veya direkt olarak sempatizanları ile iletişim kurabilmektedirler.<sup>40</sup>

---

<sup>40</sup> Brigitte Nacos, **a.g.e.**, s.4.

## ÜÇÜNCÜ BÖLÜM

### TERÖR

#### 1. Geleneksel Terör ve Terörizm Kavramları

Terör, genellikle dini, ekonomik, etnik kökenli veya siyasi bir dava uğruna girişilen, toplumu korkutmaya, yıldırmaya, sindirmeye ve sosyal hayatı durdurmaya yönelik belirli bir kişi veya örgütün yaptığı şiddet eylemidir. Buna ek olarak gücünü ve yetkilerini bu amaçla doğrudan kullanarak devlet terörizmi ya da iktidara sahip olanların kendi çıkarları doğrultusunda kullandığı örgütlere verdiği desteği ifade eden devlet destekli terörizm kavramları da terör kavramının içinde yer almaktadır. 3713 sayılı Terörle Mücadele Kanunu'nun birinci maddesinde;

*“Terör; baskı, cebir ve şiddet, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetinin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü eylemlerdir”<sup>41</sup>* şeklinde tanımlanmaktadır.

---

<sup>41</sup> T.C.Resmi Gazete, 12 Nisan 1991, Sayı:20843, s.1.

Bir başka kaynakta ise terör; “*şiddet kullanma ya da şiddet tehdidi içeren normal dışı yollarla siyasal davranışı etkilemek üzere tasarlanmış sembolik nitelikte bir fiildir*” şeklinde tanımlanmaktadır.<sup>42</sup> Terörizm ise şiddetin sistemli bir şekilde uygulandığı/kullanıldığı bir yöntem olarak aşağıdaki özelliklere sahip olduğu belirtilmektedir.<sup>43</sup>

- \* Önceden planlıdır ve toplum üzerinde korku iklimi yaratmak amaçlanmıştır.
- \* Aslında ilk kurbanlardan çok daha geniş bir kurban kitlesi hedeflenmiştir.
- \* Saldırıları askeri unsurların yanı sıra doğrudan sivilleri de hedef alır.
- \* Normal dışı yöntemler kullanılır.
- \* Özellikle devlet yetkililerinin siyasi davranışlarını etkileyerek kendi lehine kamuoyu oluşturmak için kullanılır.

Yukarıda da açıklandığı gibi terör kavramı dehşet, şiddet ve korkuyu içerirken, terörizm kavramı olaylara siyasi nitelik ve süreklilik katmaktadır. Bu bağlamda terörizm; “*Savaş ve diplomasi ile kazanılmayan sonuçları elde etmek, korkutmak ve itaat ettirmek için bir teoriye, felsefeye ve ideolojiye dayanılarak siyasi maksatlarla, iradi olarak terör ve şiddetin sistemli ve hesaplı bir şekilde*

---

<sup>42</sup> Thomas Perry Thorton, **Terror as a Weapon of Political Agiation: Internal War**, Ed:Harry Eckstein, The Free Press, New York 1964, s.73.

<sup>43</sup> Paul Wilkinson, **Terrorism versus Democracy**, Routledge, London 2006, s.1.



*kullanılmasıdır*<sup>44</sup> şeklinde en geniş tanıma sahip olur. Sonuç olarak terör silahlı eylemler vasıtasıyla kendini ve ülküsünü dünyaya duyurma amacıyla gizlice yapılan stratejik eylemleri içerirken, terörizm terör faaliyetlerini savunma, stratejileri anlatma, stratejileri geliştirme üzerine kurulu stratejik söylemlerden oluşan düşünce akımıdır.<sup>45</sup> Bu noktadan hareketle, eylemden sonra ortaya çıkan yansımaların eylem ile karşılaştırıldığında çok daha fazla etki uyandırdığı görülecektir. Bu kapsamda terörizmin nihai amacı, devletin veya toplumun herhangi bir unsuruna yöneltilecek bir saldırı hedefinin can ve mal kaybına sebep olmak veya devlet hizmetlerinin aksatılması amacıyla değil, kitlerin gözünde devlet ve güvenlik unsurlarını küçük düşürmek, toplumda güvensizlik, endişe ve korku duyguları yaratmaktır.<sup>46</sup> Bu bağlamda Resim 5, 17 Şubat 2016 tarihinde Ankara’da ve 1 Mayıs 2016 tarihinde Diyarbakır’da gerçekleştirilen terör saldırıları sonrasında kaydedilen durumu yansıtmaktadır.



(a) Ankara Saldırısı



(b) Diyarbakır Saldırısı

**Resim 5 – Terör Saldırısı Sonrası Görüntüler**<sup>47</sup>

<sup>44</sup> <http://egm.gov.tr/temuh/terorizm1.html> (Erişim Tarihi 29.09.2020).

<sup>45</sup> Gizem Özkışlalı, **Küreselleşme, İnternet ve Terörizmin Değişen Yüzü; Siber Terörizm**, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara 2008, s.49.

<sup>46</sup> Haydar Çakmak ve Cenker Korhan Demir, **Siber Dünyadaki Tehdit ve Kavramlar: Suç, Terör ve Savaş Üçgeninde Siber Dünya**, Ed: Haydar Çakmak ve Taner Altunok, Barış Platin Kitabevi, 1. Baskı, Ankara 2009s.35-37.

<sup>47</sup> [www.amp.dw.com](http://www.amp.dw.com) (Erişim Tarihi: 07.11.2020).

## 2. Terör Örgütleri ve İnternet

Terör örgütleri, ideolojilerini yaymak, sempatizanlar kazanmak, üyelerini eğitmek ve eylemlerinde kullanacakları araçları temin edebilmek için mali kaynaklara ihtiyaç duymaktadırlar. Dolayısı ile eylemlerden önce istedikleri etkiyi oluşturmada kullanacağı silah ve silah sistemlerini elde edebilmek ve eylem anına kadar gizlenmek için bir finansöre ihtiyaç duymaktadırlar. Bu finansör başka bir devlet olabileceği gibi, uyuşturucu ve silah kaçakçılığı gibi eylemlere katılarak bizzat örgütün başka bir kolu da olabilmektedir. Görüldüğü üzere geleneksel terör eylemleri için oldukça büyük kaynaklara ihtiyaç duyulmaktadır.

Gerçek dünyanın aksine sanal dünya terör örgütlerine düşük maliyetli silah sistemleri, büyük kitlelere hitap edebilme, yeni sempatizan ve üye kazanma, fon sağlama, istihbarat toplama, yüksek gizlenme araçları ve en önemlisi istedikleri etkiyi yaratabilme imkânı sağlayacak bir ortam sunmaktadır.<sup>48</sup> Timothy L. Thomas, Amerikan Ordusu'na ait Parameters adlı yayında terör örgütlerinin neden interneti kullanmayı tercih ettiğini aşağıdaki şekilde sıralamıştır.<sup>49</sup>

- \* Tüm sempatizan ve militan profillerinin toplanmasına imkân vermektedir.
- \* Gerçek bir ideolojik silah olarak kullanılabilir.

---

<sup>48</sup> Taner Altunok ve Aşkın İnci Sökmen, ‘‘Dünya’dan Siber Terör Örnekleri’’, **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, Ed: Haydar Çakmak ve Taner Altunok, Barış Platin Kitabevi, Birinci baskı, Ankara 2009, s.94.

<sup>49</sup> Timothy L. Thomas, ‘‘Al Qaeda and the Internet: The Danger of Cyberplanning’’, **Parameters (Report)**, Cilt:23, Sayı:1, Bahar 2003, s.119-121.

- \* Bir web adresinin başka başka ülkelerde yeniden oluşturulabilmesi örgüte kolay yayılma imkânı sunmaktadır.
- \* Yanlış bilgilendirme yaparak kamuoyunu kolaylıkla yanıltma imkânı sunmaktadır.
- \* Örgüt için hayati öneme haiz finans kaynaklarına internet üzerinden pazarlama yoluyla ulaşma imkânı sağlamaktadır.
- \* İnternetin dışarıdan kontrol edilebilir ve talimat verilebilir bir yapıya sahip olması emir komutayı kolaylaştırmaktadır.
- \* İnternette ideolojilerin kolaylıkla yayınlanabilmesi çok fazla çaba sarf etmeden sempatizan kazanımı sağlamaktadır.
- \* İnternet, potansiyel hedefler için istihbarat toplama imkânı sunmaktadır.
- \* İnternet, eylem alanına yaklaşmak zorunluluğunu ortadan kaldırmaktadır.
- \* İnternet, bilgi hırsızlığı veya veri değiştirme imkânı sunmaktadır.
- \* İnternet, diğer üyeler veya sempatizanlarla iletişimde gizli mesajların gönderilmesine imkân vermektedir.
- \* İnternet, terör örgütünün az kaynakla dünyanın her yerine ulaşabilmesine ve propagandasına küresel kamuoyu oluşturabilme imkânı sunmaktadır.
- \* İnternet, terör örgütünün tüm üye, sempatizan veya destek vermek isteyen hackerleri bir eylem için kolaylıkla organize etme imkânı sunmaktadır.

- \* Terör örgütü, internetin küresel ve uluslararası kurallarının kendi çıkarlarına kullanabilmektedir.
- \* İnternet, daha önce başka bir yerde yaşanmış gerçek olayların hedef ülkede tekrar yapılabilmesine imkân vermektedir.

Resim 6'da klasik kolluk güçleri tarafından yapılan baskınlar neticesinde elde edilen klasik terör malzemeleri ve siber terör malzemeleri gösterilmektedir. Bu iki fotoğraf arasında kolluk güçleri tarafından yapılan baskın neticesinde elde edilen klasik terör malzemelerinin maliyeti ile siber terör malzemeleri fiyatı karşılaştığında terör örgütlerinin halkta infial uyandıracak eylemler için neden siber uzayı tercih ettikleri daha iyi anlaşılacaktır.



(a) Klasik Terör Malzemeleri

(b) Siber Terör Malzemeleri

**Resim 6** – Kolluk Güçleri Tarafından Ele Geçirilen Terör Malzemeleri<sup>50</sup>

### 3. Terör Örgütlerinin İnternet Kullanımı

Teröristler, internet'i terörist amaçlarla kullanmaktadırlar. Yine de bu amaç, devam eden ve çatışmalı bir tartışmaya tabidir. Çünkü bazı

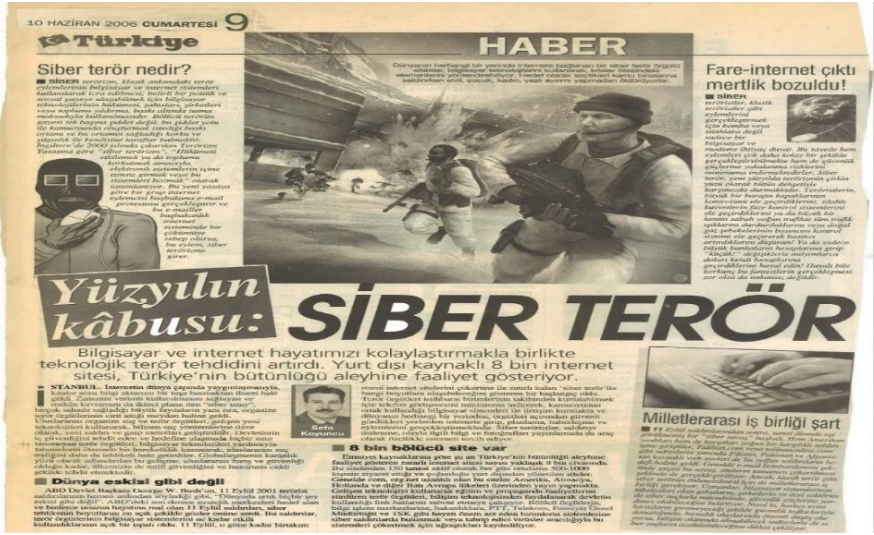
<sup>50</sup> www.haberler.com (Erişim Tarihi: 07.11.2020).

yazarlar veya uzmanlar, bugüne kadar, tek bir siber terörizm vakasının kaydedilmediğini iddia ederken, diğerleri teröristlerin zaten rutin olarak interneti kullandığını iddia etmektedirler. Bu görüş farklılıklarının temel nedeni, "terörizm" ve "siber terörizm" kavramlarının altında yatan terimlerin iyi tanımlanmamasıdır.<sup>51</sup> Nitekim 1988 yılında yapılan bir çalışmada 20'den fazla tanımsal unsuru olan 100'den fazla farklı terörizm tanımı tespit edilmiştir.<sup>52</sup> Resim 7'de, 2006 yılında Sefa Koyuncu'nun kaleme aldığı habere bakıldığında siber terör yüzyılın kâbusu olarak nitelendirilmektedir. Çünkü özellikle "siber terörizm" tanımlarına bakıldığında internetteki diğer sistemlere saldırmak için internet'i kullanmak ve bu sayede kişilere veya mülke karşı şiddete neden olmak gibi dar bir tanımdan, teröristler tarafından silah gibi kullanılması şekli de dâhil olmak üzere çok geniş bir çerçevede değiştiği görülmektedir. Sonuç olarak, teröristler eylemlerini uygulamaya geçirmekte interneti kullandıklarında birçok avantaj elde etmektedirler.

---

<sup>51</sup> Ben Golder ve Williams George, "What is Terrorism? Problems of Legal Definition", **University of New South Wales Law Journal**, Cilt: 27, Sayı: 2, 2004, s.270-295.

<sup>52</sup> Jeffry Record, **Bounding The Global War on Terrorism**, Strategic Studies Institute, US Army War College, Aralık 2003, 64 s.



Resim 7 – Terör Örgütleri İnternet Kullanımı<sup>53</sup>

Teröristler, interneti esas olarak üç farklı alanda kullanmaktadır. Birincisi, gazete veya televizyon haberlerine bakıldığında, internet üzerinden gerçekleştirilen terör saldırılarının özellikle “siber terörizm” olarak değerlendirildiği görülmektedir. Bu haberlerde yer alan saldırılar ya bireysel bilgisayarlar aracılığı ile ya da merkezi sunucular ve yönlendiriciler gibi diğer Bilişim Teknolojileri alt yapılarına, akıllı binalara, uçuş kulesine ve uçaklara, trenlere ve tren yollarına ve hatta doğrudan can kaybını hedef almaktadırlar. İkincisi, yoğun bir şekilde gözlemlenen ve korkutucu olan bu saldırıların yanı sıra, teröristler interneti sadece kayıp verdimek için kullanmazlar. Küreselleşen dünyada internet erişimi birçok ülkede mevcut olduğu için, terör örgütleri interneti yalnızca saldırmak için değil, aynı zamanda bilgilendirmek, tehdit etmek ve dikkat çekmek için de

<sup>53</sup> Sefa Koyuncu, “Siber Terör”, Türkiye Gazetesi, 10 Haziran 2006.

kullanılmaktadırlar. Son olarak, İnternet pek çok olasılık ve bilgi gibi diğer tüm kullanıcılarına sağladığı imkânları teröristlere de sunmaktadır. Bu olasılıklar, sansür ve kitlesel gözetimin uygulandığı ülkelerdeki insanlar arasında şifrelenmiş bilgi alışverişini ve olası hedefler hakkında bilgi edinmeyi içermektedir.

İnternet faktörü toplum hayatını kolaylaştırmakla birlikte menfaat odaklı kişi veya gruplar, terör örgütleri ve diğer devletler yüzünden korkulu bir rüya halini de almaktadır. Çünkü devletlere zarar vermek niyetinde olan kötü amaçlı kişiler eyleme özellikle kalabalık yerlerde, tören ve festivallerde toplumu oluşturan sıradan kişileri hedef almaktadır. Bunun yanı sıra, gelişen teknoloji ile küreselleşmenin artması bahse konu terör örgütleri için kıtalar arası eylemleri gerçekleştirmeyi bir tuşa basacak kadar kolay hale getirmektedir. Sağladığı kolaylıklar ve fark edilme ihtimalinin düşüklüğü siber uzay olarak tarif edilen internet ortamını terör örgütlerinin cirit attığı bir ortam haline getirmiştir. Hedeflerine ulaşmada ve ideolojilerini yaymada hiçbir sınır tanımayan terör örgütleri bilgisayar ve internet sayesinde tahmin dahi edilemeyen bir hareketlilik kazanmakta ve ulusal ve uluslararası terör eylemlerini daha tehlikeli hale getirmektedir. Bu bağlamda küreselleşmenin karanlık tarafını faal olarak kullanma gayreti içerisinde olan terör örgütleri tüm ulusların güvenliğini ve uluslararası barışı ciddi şekilde tehdit etmektedirler.

### **a. İnternet Üzerinden Terör Saldırıları**

İnternet, oldukça uzun süredir, özellikle parasal gelir elde etmek isteyen çıkar gruplarının sistemleri kendi çıkarları için kötüye

kullandığı siber suç alanı olmuştur. Ancak unutulmaması gereken şudur ki, bu eylemler sadece çıkar amaçlı değil aynı zamanda terörist niyetle de işlenebilmektedir. Terör örgütlerinin eylemlerini neden siber uzayda gerçekleştirdiğini tespit edebilmek için öncelikle eylemin arkasındaki nedenlere ve güdülere bakmak gerekmektedir. Çünkü internet üzerinden gerçekleştirilen terör saldırıları genel anlamda oldukça esnektir ve birkaç farklı şekilde birleştirilebilmektedir. Örneğin, belirli bir bilgisayar sisteminin güvenliğini “test etmek” amacıyla gerçekleştirilen bir bilgisayar korsanlığı saldırısını, sistemi kapatmak ve daha fazla hasar oluşturmak için gerçekleştirilen başka bir bilgisayar korsanlığı saldırısından ayırt etmek oldukça zordur. Bununla birlikte, terörist hırslarla ilgili olarak, saldırılar Bilişim Teknoloji alt yapı sistemlerine ve doğrudan insan hayatına yönelik olarak iki gruba ayrılmaktadır.

İnternet üzerinden gerçekleştirilen birçok saldırı, arkasındaki nedenlerle ilgili hiçbir açıklama yapmadığından, olayın organize bir grubun terör eylemi olup olmadığını belirlemek çoğu zaman mümkün olmamaktadır. Bu bağlamda, birçok siber saldırı vakasında, kaynağın ne, kim ya da kimler olduğu tespit edilememektedir. Yukarıda da belirtildiği üzere bu nedenle, bazı yazarlar, şimdiye kadar, tek bir siber terörizm vakasının kaydedilmediğini iddia etmektedirler.<sup>54</sup> Aslında gayri resmi kaynaklara göre pek çok siber-terör saldırısının hâlihazırda gerçekleşmektedir; ancak, önemli altyapılara yönelik

---

<sup>54</sup> Ulrich Sieber, The Threat of Cybercrime, In Council of Europe (Ed.), Organised Crime in Europe, **Strasbourg: Council of Europe Publishing**, Situation Report 2004, Bölüm 3, s.81-218.



güvenlik tehdidi nedeniyle birçok vaka (çoğu değilse de büyük bir bölümü) gizli tutulmakta olduğu değerlendirilmektedir. Bununla birlikte, teröristlerin interneti kendi amaçları için kullanmaları tehdidi gerçekçi olmadığı düşünülse de her an siber saldırı yapılabileceği korku ve çaresizlik duygusu yaratmak bir tür psikolojik savaş olarak kullanılabilir. <sup>55</sup>

Pek çok farklı neden ve güdünün varlığı, İnternet'in genel olarak neden sadece “sıradan” suçlular için değil, aynı zamanda terörist amaçlar için de ilginç olduğunu göstermektedir. Philip W. Brunst çalışmasında bu nedenleri şu şekilde belirtmektedir: <sup>56</sup>

- \* İnternet üzerinden gerçekleştirilen saldırılar dünyanın her yerinden başlatılabilmektedir. Klasik bir bombalı saldırıda olduğu gibi eylemin gerçekleştirileceği yerde olmak gerekli değildir. Saldırının başlatılması için gerekli olan internet bağlantıları yaygın olarak mevcuttur. Çünkü çoğu saldırı cep telefonu vasıtası ile başlatılabilmektedir.
- \* Saldırı neredeyse hiç hazırlık yapmadan hızlı bir şekilde başlatılabilmektedir. Bu sayede güncel olaylara karşı anında tepki verilebilmektedir.
- \* Birçok saldırı türünün hızı, saldırganın bağlantı hızına bağlı değildir. Ancak saldırıya uğrayan kişi veya kurum kendi

---

<sup>55</sup> Gabriel Weimann, “‘www.terror.net: How Modern Terrorism Uses the Internet’”, **United States Institute of Peace**, Special Report 116, Mart 2004, s.5.

<sup>56</sup> Phillip W. Burnst, **Use of the Internet by Terrorists-A Threat Anallyis: Responses to Cyber Terrorism**, Edited by Centre of Excellence Defence Against Terrorism, Ankara Turkey, IOS Press, Amsterdam 4-5 October 2007, s.35-40.

bilgisayarlarının bağlantı hızının kurbanı olmaktadır. Böylece, solucanlar ve virüsler, saldırının daha fazla müdahalesine ve zaman harcamasına gerek kalmadan mümkün olan en hızlı şekilde yayılmaktadırlar.

\* İnternet üzerinden gerçekleştirilen eylemler anonim ve izlenemez durumda tutulabilmektedir. Teknik olarak, anonimleştirme hizmetleri ve benzeri kamufle etme tekniklerinin yanı sıra diğer saldırıya uğramış sistemler aracılığıyla trafiğin iletilmesi, bir saldırının izlenmesini imkânsız değilse de oldukça zor bir hale getirmektedir. Dahası, izler farklı ülkeler üzerinden yürütülürse, bu ülkelerdeki yasal sorunlar ve farklı teknik standartlar zorluklar listesine eklenir. Son olarak, dijital kanıtlar kasıtlı olarak taklit edilebildiğinden dolayı olaya karışmamış masum taraflara karşı şüphe uyandırabilmektedir.

\* Maliyet-fayda oranı son derece olumludur, çünkü internet kullanımı son derece ucuzdur. Çoğu saldırı için neredeyse dünyanın her yerinde ulaşılabilen yalnızca küçük bir bant genişliği bağlantısına ihtiyaç vardır. Bu ucuzluğun karşısında, internet yoluyla verilen hasar oldukça maliyetli olabilir. Ayrıca, saldırı sadece fiziksel zarar vermekle kalmaz ve Bilişim Teknolojileri uzmanları tarafından yeni keşfedilen güvenlik kusurlarının giderilmesine yönelik büyük bir bütçe harcanır.

\* Çoğu hedef zayıf bir şekilde korunduğundan saldırıların gerçekleştirilmesi kolaydır. Bu nedenle, saldırganlar çok sayıda ve çeşitte savunmasız hedefler arasından seçim yapabilir. Tercih edilen

hedef “tercih edilen silaha” karşı savunmasız değilse, diğer birçok hedef hala mevcut olmayı sürdürmektedir.

### **b. Terör ile Bağlantılı İçerikler**

İnternetin büyük gücü, her zaman iletişim için kullanılması olmakla beraber asıl başarı www'nin kurulması ve herkesin bilgi yayma imkânına sahip olması ile gerçekleşmiştir. Bu bağlamda, günümüzde teröristler interneti yalnızca saldırıları başlatmak için değil, aynı zamanda interneti “fikir savaşında” yeni olanaklar için de kullanmaya başlamışlardır.<sup>57</sup> İnternetin kullanımı, özellikle terörist bakış açılarının sunulması, tehdit ve propaganda yapılması ve bunun için kaynak yaratma olasılığının azlığı açısından oldukça ilgi çekicidir.

#### **(1) Terörist Bakış Açısının Sunumu**

Geleneksel teröristler ve terör örgütlerinin gizli çalışmak zorunda olmaları görüşlerinin, amaçlarının ve hırslarının iletişimini son derece zorlaştırmaktadır. Çünkü eski usullerle fikir yaymanın geleneksel yolları, broşürler ve kulaktan kulağa propagandadır. Ancak her iki alternatif de oldukça zaman alıcıdır ve bir o kadar da riskli olmasına karşın geniş bir kitleye ulaşmayı garanti etmezler. Buna ek olarak, teröristler medyayla veya bu tür bilgileri aktif olarak aramayan ancak bir kez tanıtıldıktan sonra ilgisini çekebilecek diğer kişi ve kuruluşlarla nasıl iletişim kurulacağı sorunuyla karşı karşıyadırlar.

---

<sup>57</sup> Giampiero Giacomello, “Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism”, *Studies in Conflict & Terrorism*, Cilt: 27, Sayı:5, 2004, s.387-408.

İnternetin yardımıyla tüm faaliyetlerin değiştiği gibi terörizm usulleri de değişmiştir. Çok önceleri propaganda faaliyetleri için televizyon, radyo ve basılı yayın organlarını kullanan terör örgütleri internetin yaygınlaşması ile beraber ilgi alanını bu yöne kaydırmış ve gün geçtikçe terör örgütlerinin kendi web sitelerinde kayda değer bir artış gözlenmiştir.<sup>58</sup> Amerika Birleşik Devletleri Bakanlığı'na (United States Department of States) göre 1999'da 30 yabancı terör örgütünden on ikisinin kendi web siteleri varken<sup>59</sup>; Gabriel Weimann 2005 yılında bazıları Tablo 2'de gösterilen 4.500'den fazla teröristle ilgili web sitesinin izini sürmüştür.<sup>60</sup> Birçok web sitesi örgütün liderini, kuruluşun geçmişini, amaçlarını veya son başarılarını ayrıntılı bir şekilde yayınlamaktadırlar. Hatta bazı web siteleri, gençlere ulaşmak için sohbet odaları, siberkafeler gibi interaktif internet teknolojilerini kullanmaktadırlar.<sup>61</sup> Ayrıca, bazı terör web siteleri, yabancıların bile medya haberlerini ilgili kuruluşun görüşleriyle karşılaştırabilmeleri için farklı dillerde bilgi sağlamaktadır. Örneğin Tablo 2'de gösterildiği üzere Kolombiya Devrimci Silahlı Kuvvetlerinin web sitesi İngilizce, İspanyolca, İtalyanca, Portekizce, Rusça ve Almanca bilgiler sunmaktadır.<sup>62</sup>

---

<sup>58</sup> Weimann, **a.g.m.**, s.6.

<sup>59</sup> Maura Conway, "Reality bytes: Cyberterrorism and Terrorist "use" of the Internet", **Department of Political Science**, Cilt: 7, Sayı: 11, 2002, s.3.

<sup>60</sup> Steve Coll ve Susan B. Glasser, Terrorists Turn to the Web as Base of Operations, **The Washington Post**, 7 Ağustos 2005.

<sup>61</sup> Weiman, **a.g.m.**, s.8.

<sup>62</sup> Conway, **a.g.m.**, s.4.

Terör Örgütü	İnternet Adresi (URL)	Dili
Aum Supreme Truth (Aum)	www.aleph.to/index e.html www.aleph.to	İngilizce Japonca
Basque Homeland and Liberty (ETA)	www.contrast.org/mirrors/ehj/index www.batasuna.org/	İngilizce Baskça
Al-Gama'a al Islamiyya (Islamic Gr.)	www.azzam.com	İngilizce
Hizbollah	www.hizbollah.org	Arapça İngilizce
Kursidtan Workers Party (PKK)	www.pkk.org/index.html	Kürtçe
Lashkar-e Tayyiba	www.markazdawa .org.pk/	Arapça İngilizce
Palestine Islamic Jihad (PIJ)	www.entifada.net/	Arapça
Al-Qaida	www.alneda.com	Arapça
Revolutionary Armed Forces of Colombia (FARC) (Kolombiya Devrimci Silahlı Kuvvetleri)	www.farc.ep.org	İngilizce İspanyolca Portekizce İtalyanca Almanca Rusça
Revolutionary People's Liberation Party/Front (DHKP/C, Dev Sol)	www.ozgurluk.org	İngilizce

**Tablo 2** – Bazı Web Sitesi Olan Terör Örgütleri ve Yayın Yaptıkları Diller

Teröristler web sitelerinde içerikle ilgili olarak sadece örgütleri hakkında bilgi sunmakla sınırlı kalmamaktadırlar. Sadece bakış açılarının sunulmasından terörizmin yüceltilmesine veya son şiddet eylemlerinin veya sıradaki tehditlerinin gerçekleştirilmesine, okuyucular, dinleyiciler ve yeni üyeler tarafından daha fazla terörist eylemi kışkırtmaya kadar her şey neredeyse mümkündür. Hatta ölülerinin onurlandırılması ve teröristlerin aileleriyle iletişim kurmaları çok uzun süredir uygulamada olan bir durumdur. Örneğin alneda.com web sitesi, yakalanan 84 El Kaide savaşçısının(!)

isimlerini ve ev telefon numaralarını yayınlamıştır.<sup>63</sup> Muhtemelen, bu eylemin amacı sempatanların aileleriyle iletişim kurmalarına ve hayatta olup olmadıklarını bildirmelerine izin vermektir. Diğer web siteleri ise intihar bombacılarının ölüm ilanlarını içermekte, onları etkili bir şekilde yüceltip ve başkalarını bu yolu izlemeye teşvik etmektedir.<sup>64</sup> Bu nedenlerle İnternet, terör örgütlerinin destekçileri ve diğer ilgili taraflarla iletişim kurduğu en önemli araç haline gelmiştir.

En popüler terör siteleri her ay on binlerce ziyaretçiyi çekmektedir.<sup>65</sup> Elbette hükümetler bu tür web sitelerini kapatmaya ve bilginin yayılmasını önlemeye çalışmaktadırlar. Yine de internetin sansür direnci kavramı sıklıkla kullanılmaktadır. Örneğin, Ürdünlü yetkililer The Economist'in Ürdün'de satışa sunulan 40 basılı nüshasından bir makale çıkarmış, çevrimiçi bir kopya basımını yapmış, tıpkıçekimini yapıp 1.000 Ürdünlüye belge geçerek yerel sansürlerin önüne geçebilmişlerdir.<sup>66</sup> Ayrıca, web siteleri genellikle, kuruluşun faaliyet gösterdiği ülkeden farklı başka bir ülkede fiziksel olarak bulunan sunucularda saklanmaktadır. Örneğin, El Kaide'nin birkaç web sitesi ABD ve Kanada'da fiziksel olarak saklanmaktadır.<sup>67</sup>

---

<sup>63</sup> Burnst, **a.g.e.**, s.46.

<sup>64</sup> Von Yassin Musharbash, Terrorism in the Internet: The Cyber-Cemetery of the Mujahedeen, **Spiegel International**, 28 Ekim 2005.

<sup>65</sup> Conway, **a.g.m.**, s.6.

<sup>66</sup> Dorothy E. Denning, "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool For Influencing Foreign Policy Decision Making", **Network and Netwars: The Future of Terror, Crime and Militancy**, Sekizinci Bölüm, Ed.: John Arquilla ve David Ronfeldt, Rand Corporations, San Francisco 1999, s.243

<sup>67</sup> Burnst, **a.g.e.**, s.47.

## (2) Terör Örgütlerinin Tehdit ve Propaganda Aracı Olarak İnternet

Terörist web siteleri yalnızca görüşlerin sunumuyla sınırlı kalmamakla birlikte düşmanlara tehdit göndermek ve propaganda yaymak için de kullanılmaktadır. Örnek olarak Afganistan'daki Alman ve Avusturya'ya yönelik tehdit videoları verilebilir. Videolar Global Islamic Mediafront (GIMF) adlı bir web sitesine gönderilmiştir. Alman Anayasayı Koruma Bürosunun üst düzey yetkilileri bu videonun bir "psikolojik savaş" biçimi olarak görüldüğünü çünkü doğrudan tehdit oluşturmadığını, bunun yerine bir huzursuzluk ortamı yarattığını söylemiştir.<sup>68</sup>

Teröristler, YouTube gibi video paylaşım platformlarına birçok propaganda videosu yükleyerek propagandadan etkilenen veya örgütün görüşlerine açık olan ancak aktif üye olmayan sempatizanları tespit etmek için de kullanılabilir hale getirmektedir. Bu videolarda terörizm muhteşem bir olguymuş gibi lanse edilmekte ve saldırı sahneleri müzik eşliğinde sunulmaktadır.

İnternetin gelişimi ile birlikte geçmişte sadece birkaç köklü kuruluş gazete, dergi veya TV şovu üretebiliyorken, günümüzde her birey bu işlemi gerçekleştirebilmektedir. Çünkü internet geleneksel kitle iletişim araçlarına göre maliyet avantajı sağlamakta ve bu tür yayınların tanıtımına büyük ölçüde yardımcı olmaktadır. Örneğin El

---

<sup>68</sup> A.g.e., s.48.

Kaide, terörist bir bakış açısından dünya haberlerini içeren haftalık iki dilli bir haber programı başlatmıştır.<sup>69</sup>

### **(3) Terör Örgütlerinin Finansman Aracı Olarak İnternet**

Siyasi, felsefi, dini vb. amaçlı birçok kurum, kuruluş veya örgütler web sitelerini sadece bilgi yaymak için değil, aynı zamanda finansman için bir gelir kaynağı olarak (kaynak yaratma) kullanmaya başlamışlardır. Bu tip kaynak yaratma işlemleri genellikle CD, DVD, tişört, rozet, bayrak, kitap vb. satarak yapılmaktadır. Bazı web siteleri ise doğrudan kredi kartı yoluyla veya banka hesabı ayrıntılarını sağlayarak kurum veya kuruluşa nasıl para bağışlanacağına dair talimatlar vermektedirler. Bunu yapan kurum ve kuruluşlar, sempatizan, destekçiler ve muhtemel örgüt adayları ile bağlantı kurmayı amaçlamaktadırlar. Muhtemel örgüt adayları olarak belirlenen kullanıcılar ile daha sonra e-posta yoluyla tekrar iletişime geçilip daha fazla bağış yapmaları istenmektedir.

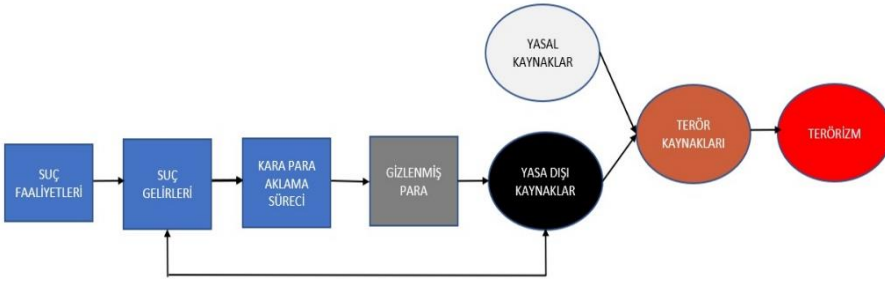
Diğer birçok siyasi örgüt gibi, terör örgütleri de finansman sağlamak için interneti kullanmaktadırlar. Örneğin El Kaide, her zaman büyük ölçüde bağışlara bağımlı olmuştur ve küresel bağış toplama ağı, hayır kurumları, sivil toplum kuruluşları ve web siteleri ile internet tabanlı sohbet odaları ve forumları kullanan diğer finans kurumlarının temeli üzerine kurulmuştur.<sup>70</sup> Sünni aşırılık yanlısı grup Hizb al-Tahrir, destekçilerinden para vererek ve diğerlerini cihat davasına bağışta

<sup>69</sup> Musharbash, a.g.g.

<sup>70</sup> Weimann, a.g.m., s.7.



bulunmaya teşvik ederek çabalara yardım etmelerini isteyen, Avrupa'dan Afrika'ya uzanan entegre bir İnternet siteleri ağı kullanmaktadır.<sup>71</sup> Bunun gibi birçok usulle para toplamaya çalışan terör örgütlerinin banka bilgileri ise genellikle başka ülkeler üzerinden sunulmaktadır. Örneğin Hizb al-Tahrir'in bağış topladığı banka hesap bilgileri Almanya merkezli bir sitede sunulurken, Rusya'dan ayrılan Çeçenya Cumhuriyeti'ndeki savaşçılar da benzer şekilde, sempatizanların katkıda bulunabileceği banka hesaplarını Kaliforniya ve Sacramento üzerinden duyurmaktadır. Şekil 4'te terör örgütlerinin kaynak yaratma süreci gösterilmektedir.



Şekil 4 – Terör Örgütlerinin Finansman Sağlama Süreci<sup>72</sup>

#### (4) Terör Örgütlerinin Örgüte Yeni Üye Alma Aracı Olarak İnternet

İnternet sadece sempatizanlardan bağış istemek için değil, aynı zamanda destekçileri terörist faaliyetlerin veya amaçların desteklenmesinde daha aktif bir rol oynamaya teşvik etmek için de

<sup>71</sup> A.g.m., s.8.

<sup>72</sup> Hamed Tofangsaz, “A New Approach to the Criminalization of Terrorist Financing and Its’ Compatibility with Sharia Law”, **Journal of Money Laundering Control**, Cilt: 15, Sayı:4, Ekim 2012, s.401.

kullanılabilir. Terör örgütleri, mesajlarının yayını iyileştirmek için web sitesi teknolojilerinin (ses, dijital video, vb.) tüm yelpazesini kullanarak dönüşüm arayışına ek olarak, web sitelerinde gezinen kullanıcılar hakkında bilgi toplamaktadırlar. Örgütün amacına en çok ilgi duyan veya işini yürütmek için çok uygun görünen kullanıcılarla daha sonra iletişime geçerler. Örgüte yeni üye kazandırma görevlileri ayrıca çevrimiçi sohbet odalarında ve siber kafelerde dolaşmak için daha etkileşimli İnternet teknolojisini kullanmakta ve özellikle genç insanlar olmak üzere toplumda teröre meyilli bireyleri tespit edebilmektedirler.

Bazen ise bizzat aday üyelerin kendilerini terör örgütlerine tanıtmak için interneti kullandığı durumlar tespit edilmektedir. Örneğin, 1995 yılında Verton tarafından Black Ice'ta bildirildiği üzere, Ziyad Khaleel Missouri'deki Columbia Koleji'nde bilgisayar bilimleri okulu kampüsünde önce Müslüman bir aktivist olmuş, birkaç radikal grupta bağlantı kurmuş, Hamas'ı destekleyen bir web sitesi işletmiş ve bu sayede Usame Bin Ladin ve yardımcılarının dikkatini çekerek ABD'deki El Kaide'nin uydu telefon, bilgisayar ve diğer elektronik gözetim teknolojileri satın alma görevlisi olmuştur.<sup>73</sup> Resim 8'de Bill Warner'in internette bulunan tek fotoğrafı ile Ziyad Khaleel'i tanıtmaya yer almaktadır.

---

<sup>73</sup> Weimann, a.g.m., s.8.



Resim 8 – Terörist Ziyad Khaleel<sup>74</sup>

<sup>74</sup> Bill Warner, “Bill Warner Investigations Sarasota:Al-Qaeda Agents Anwar al-Awlaki, Ziyad Khaleel & Muneer Arafat Part of 9/11 Hijackers Support Network in U.S.”, 21 Ocak 2019. [www.billwarnerpi.com](http://www.billwarnerpi.com) (Eriřim Tarihi: 07.11.2020).

## DÖRDÜNCÜ BÖLÜM

### SİBER GÜVENLİK VE SİBER TERÖRİZM

Güvenlik kavramı, tüm kurumlar için iki farklı tür önlemleri ifade etmektedir. Bunlardan ilki çalışanların çalıştıkları kuruma bilinçli veya bilinçsiz bir şekilde zarar verici eylemlerde bulunmasını önleme amaçlıdır. İkincisi ise kurum ile bağlantısı olmayan saldırgan veya teröristlerin kuruma zarar verici eylemlerde bulunmasını önleme amaçlıdır. Her iki tür kavramda da ana hedef kurum için kritik değere sahip olan bilgi, varlık ve alt yapıların fiziki olarak korunmasıdır. Bahse konu güvenlik önlemleri kapsamında çoğu kurum kendini genel ağlardan soyutlamak için kendine özel ve dışı kapalı bir ağ sistemi kurmuştur. Ancak çalışanların insani zaaflarından faydalanılarak güvenlik duvarlarını aştığı değerlendirilen ve küçük bir USB yardımıyla yerel ağa bağlanan Stuxnet Solucanı<sup>75</sup> (Stuxnet Worm) üst düzey önlemlerin alındığı sistemlerin bile yüzde yüz korunamadığını ve siber saldırıların hem kamu güvenliği hem de kurumsal hesap verebilirlik anlamında yıkıcı etkileri olabileceğini göstermiştir.<sup>76</sup>

İki dünya savaşı ve bir de Soğuk Savaş sürecini içeren yirminci yüzyıl savaşlara fiilen katılıp katılmadığına bakmaksızın tüm devletleri

---

<sup>75</sup> Tüm Dünya'da siber güvenlik sorunları hakkında farklılık yaratan Stuxnet Solucanı devletlere ve kurumlara kritik altyapıların siber saldırılara karşı savunmasız olduğunu ve olası sonuçlarının felaket olabileceğini göstermiştir. Bkz. Marie Baezner ve Patrice Robin, Hotspot Analysis: Stuxnet, Center for Security Studies (CSS), ETH Zurih, October 2017, s.4.

<sup>76</sup> Nigel Stenley, Safety and Security in Industry 4.0 – Are You Ready, <https://www.infosecurity-magazine.com/opinions/safety-industry-4-1-1/> (Erişim 15.10.2020).

üçüncü bir dünya savaşına her an hazır bulunmak durumunda bırakmıştır. Bu nedenle tüm devletler kendilerine yöneltebileceğini değerlendirdiği tehditlere karşı sürekli teyakkuzda olmak ve güvenlik protokollerini en üst seviyede uygulamak durumunda kalmıştır. Sanayi ve teknoloji açısından gelişmemiş olan devletlerin güçlü devletlerin koruması altına girme çabaları ile güçlü devletlerin çıkarları ve jeostratejik<sup>77</sup> politikaları doğrultusunda zayıf ülkeleri yanına alarak kendi güç alanını kurmaya çalışmaları dünyadaki güvensizlik ve belirsizlik seviyesini azaltmaya yönelik tedbirlerdir. Böylece devletler güvenlik kaygılarını azaltmaya, ulusal sınırlarını korumaya yönelik ikili antlaşmalara imza atmış, paktlara, cemiyetlere ve organizasyonlara katılım eğilimi göstermişlerdir. Ancak, bir yandan ittifaklar kurarak kendi güvenliklerini garanti altına almaya çalışan devletlerin kendi yanlarında yer almayan devletleri belirsizlik ve güvensizlik ortamına sürüklenme çabaları ve bunun tam tersi yönünde diğer devletlerin de kendi güvenliklerini arttırıcı önlemler ile ilk süreçte güçlü durumda olan devletleri tekrar güvensizlik ortamına itme çabaları sürekli devam eden bir güvensizlik ikilemine (security dilemma) neden olmaktadır.<sup>78</sup>

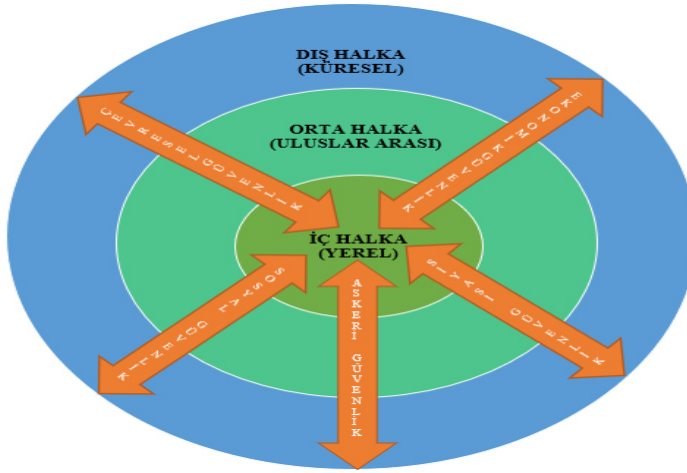
Küreselleşmenin etkisi ve bilişim teknolojilerinin hızlı gelişimi gibi nedenler eski güvenlik önlemlerinin geçerliliğini yitirmesine neden olmuştur. Bunun yanı sıra saldırıların her geçen gün daha karmaşık

---

<sup>77</sup> Jeostrateji, jeopolitiğin bir alt dalıdır. Ekonomik, politik, sosyal ve fiziki coğrafi unsurların siyasi ve askeri faaliyetlere etkilerini inceleyen ve böylece strateji ile coğrafya arasında bağı kuran bir dış politika çeşididir. Bkz. [www.coğrafya.gen.tr/siyasi/jeopolitik](http://www.coğrafya.gen.tr/siyasi/jeopolitik) (Erişim 24.10.2020).

<sup>78</sup> Güngör Şahin, **Küresel Güvenlik ve NATO Teori-Aktör-Tehdit-Risk**, Detay Yayıncılık, 2016, s.37-40.

hale gelmesi ve güvenlik açıklarından yararlananların yakalanmasının zorlaşması güvenlik tedbirleri olgusunun yeniden değerlendirilmesini gündeme getirmiştir. Böylece geçmişin fiziki güvenlik önlemleri siber güvenlik tedbirleri ile desteklenerek tüm açık kapıların kapatılmasına çalışılmıştır. Buna ilaveten gelişen teknoloji ile dünya daha küçük hale gelmekle birlikte devletlerin karşılaştığı yerel, uluslararası ve küresel tehditlerin boyutları da gün geçtikçe daha da büyümektedir. Bu bağlamda küreselleşme kavramı açısından güvenlik kavramının Soğuk Savaş sonrası değişen boyutları Şekil 5'te gösterildiği gibi ifade edilmesinin uygun olacağı değerlendirilmektedir.



Şekil 5 – Soğuk Savaş Sonrası Güvenlik Kavramının Değişen Boyutu<sup>79</sup>

## 1. Siber Güvenlik

Sibernetik kökeninden gelmekte olan siber kelimesi ilk olarak Louis Couffinal tarafından 1958 yılında canlılar ile makineler arasındaki

<sup>79</sup> Gökhan Bayraktar, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, 1. Baskı, Yenyüzyıl Yayınları, İstanbul, 2015, s.42.

iletişim disiplini tanımlamak için kullanılmıştır.<sup>80</sup> Bu kullanımda internet kavramını ifade etmede kullanılan sanal kelimesi aynı zamanda siber kelimesini de ifade etmektedir. Aralarındaki tek farkın internetin iletişim yöntemi açısından siber, yarattığı ortam açısından sanal olması şeklinde açıklanabileceği değerlendirilmektedir.

Toplum oluşturulan bireylerin korkusuzca yaşamlarını sürdürebilmeleri için devlet tarafından sağlanan bir olgu olan güvenlik kavramı gelişen teknoloji ile birlikte kapsama alanına gerçek dünya ile birlikte sanal dünyayı da almıştır. Bu bağlamda karşımıza çıkan siber güvenlik kavramı internet kullanıcısı pozisyonunda olan birey, kurum veya kuruluşların sanal ortamda varlıklarını korkusuzca devam ettirebilmeleri amacıyla alınan önlemleri kapsayan teknolojiler bütünüdür.<sup>81</sup> Bu teknolojiler bütünü herhangi bir siber saldırı anında değil, saldırıdan önce alınan tedbirleri ihtiva etmektedir. Çünkü siber saldırıda neyin saldırı olduğu algılanamamaktadır. Saldırı internet ağında kurum sırlarını çalmaktan nükleer tesis sabotajlarına kadar uzanmaktadır. Bu bağlamda ABD hükümeti 2009 yılında siber saldırıları “*bilgisayar sistemleri, ağlar veya bilgiyi ve/veya bunlarda yerleşik olan ya da bunları taşıyan programları değiştirmek, bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılmış kasıtlı hareketler*”<sup>82</sup> olarak tanımlamıştır. Dolayısı ile en iyi savunma taarruzdur yaklaşımı siber saldırılara karşı geçerli değildir. Konunun

---

<sup>80</sup> Serhat Kut, Sibermekanın Gerçekliği, <https://www.academia.edu/389859> (Erişim Tarihi: 23.12.2020).

<sup>81</sup> Atalay Keleştemur, **Siber İstihbarat**, Level Yayınevi, 1. Basım, Kocaeli 2015, s.162.

<sup>82</sup> P.W.Singer ve Allan Friedman, **Siber Güvenlik ve Siber Savaş**, Çev:Ali Atav, Buzdağı Yayınevi, 1. Baskı, Ankara 2015, s.101.

daha iyi anlaşılması açısından geleneksel saldırılar ile siber saldırılar arasındaki karşılaştırmalar Tablo 3'te sunulmaktadır.

Parametreler	Konvansiyonel Savaş	Siber Savaş
Saldırının Kaynağı	Saldırı kaynağının bulunması teknoloji sayesinde kolaydır.	Saldırının nereden geldiğini tespit etmek zordur. Kimi zamanda ispat edilememektedir.
Saldırının Hızı	Kullanılmakta olan uçak, gemi, tank, füze gibi öğelerin hızı kadardır.	İnternet hızındadır.
Etkisi	Fiziksel alanda etkisi büyüktür.	Genellikle bilgi ve iletişim sistemlerinde etkilidir. Ancak nükleer santraller vb. fiziksel etki de yaratabilmektedir.
Savaşçıları	İki veya daha fazla ülkenin orduları savaşmaktadır.	Tek bir kişi, bir grup, bir örgüt veya devlet savaşmaktadır.
Maliyeti	Kullanılan askeri silahların maliyetine bağlıdır ve genellikle oldukça pahalıdır.	Kimi zaman tek bir bilgisayar ile etkili olunabilmektedir. Maliyeti ucuzdur.
Silahları	Füze, bomba, top, tabanca, tüfek, tank, uçak, gemi, radar vb.	Bilgisayarlar, çipler, yazılımlar, donanımlar.
Teknolojisi	İleri askeri harp teknolojileri	Yüksek teknoloji ve bilgi ihtiyacı bulunmaktadır.
Saldırı belirtileri	Saldırı anında fark edilmektedir.	Saldırının farkına varılamayabilir.
Hasar tespiti	Fiziksel hasarlar kolaylıkla tespit edilebilir.	Fiziksel bir hasar olmadığı zamanlarda tespit neredeyse imkânsızdır.

**Tablo 3 – Geleneksel Saldırı ve Siber Saldırı Arasındaki Farklar<sup>83</sup>**

## 2. Siber Eylem Sınıfları

Siber eylemler farklı amaçlar için uygulanabilmektedir. Bu amaçlar ve sonucunda ortaya çıkan eylemler dikkate alındığında genel anlamda

<sup>83</sup> Telestemur, a.g.e., s.164.



siber savaş, siber casusluk, siber terör ve siber sabotaj olmak üzere dört alt başlık altında sınıflandırılabilir. Siber eylemlerin kategorilere ayrılması, motivasyon kaynakları, hedef kitleleri ve metotlarına göre Tablo 4’ te gösterilmektedir. Bu çalışmada siber eylemler, siber suç, siber saldırı, siber terör ve siber savaş olacak şekilde alt başlıklara ayrılmıştır.

	Motivasyon	Hedef Kitle	Metotlar
Siber Savaş	Askeri, Siyasi ve Ekonomik Fayda	Kritik Bilgi Sistem Altyapıları, Askeri Bilgi Sistemleri, Devletler, Kurumlar, Firmalar	Siber Taarruz Yöntemlerinin Kullanımı
Siber Casusluk	Kritik Bilgi Kazanımı, Askeri ve Ekonomik Fayda	Askeri Bilgi Sistemleri, Devletler, Kurumlar, Firmalar	Güvenlik Açıklarının Kullanımı
Siber Terör	Siyasi Fayda	Devletler	Bilgisayar Tabanlı Şiddet ve Tatmin
Siber Sabotaj	Ekonomik Fayda, Kişisel Tatmin	Devletler, Kurumlar, Firmalar	İnsan Faktörünün Kullanımı

**Tablo 4 – Siber Eylemlerin Sınıflandırılması<sup>84</sup>**

### a. Siber Suç

Teknolojinin her geçen gün gelişmesi ve buna bağlı olarak toplumsal yaşamın bu gelişmeye aynı hızda ayak uydurması insanları, kurum ve kuruluşların teknolojiye olan bağımlılıklarını arttırmaktadır. Bu bağımlılık, 30 ton ağırlığında ve 167 metre kare alanı kaplayan tarihin elektrikle çalışan ve elektronik veri işleyebilen ilk bilgisayarının (ENIAC) icadından bu yana pantolon cebine sığan bilgisayarların

<sup>84</sup> Bayraktar, a.g.e., s.51.

kullanım kolaylığı ölçüsünde artmaktadır. Ayrıca, 1945 yılında başlayıp 1947 yılında tamamlanan ENIAC'ın beş yüz bin dolara mal olduğu ve buna karşın şimdiki bilgisayarların teknoloji sayesinde daha hızlı ve daha ucuza mal edilmesi sayesinde teknolojinin yaygınlaştığı görünen bir gerçektir. Örneğin banka havaleleri, sosyal grup ilişkileri, kişisel veya kurumsal veri depolama, eğlence, alışveriş gibi işlemlerin çoğu bilgisayar ile sanal dünyada gerçekleştirilmektedir.



**Resim 9 – ENIAC<sup>85</sup>**

Bilişim teknolojilerindeki bu gelişmeler kamu veya özel kurum ve kuruluşların işlerini kolaylaştırmakta iken, vatandaş açısından da daha hızlı ve daha kaliteli hizmet alımı gerçekleşmektedir. Hayatı kolaylaştıran ve hayat standartlarını yükselten bu uygulamaların sağlıklı, hızlı, doğru ve güvenilir bir şekilde işlemesi ise hayati öneme sahiptir. Bu nedenle gerçek dünyanın yanı sıra devletler artık sanal dünyada da vatandaşlarının zarar görmesini engelleyecek önlemler

---

<sup>85</sup> Jon Fingas, “One of the First True Computers is Finally on Public Display”, 25.11.2014, [www.engadget.com/amp/2014-11-25-eniac-on-public-display.html](http://www.engadget.com/amp/2014-11-25-eniac-on-public-display.html) (Erişim Tarihi: 08.11.2020).

almaktadır. Çünkü gündelik yaşamın teknolojiye bu denli bağımlı ve teknoloji ile iç içe geçmesi insanları ve kurumları kötü niyetli kişi veya kişilerin istismarına daha açık hale getirmektedir.

Gelişen teknolojinin sağladığı kolaylıklar ve kaliteli hayat biçimi bireysel, kurumsal ve ulusal riskleri de beraberinde getirmektedir. Çünkü teknolojinin belirli bir kişi veya grubun çıkarına olacak biçimde kötüye kullanılması karşımıza yeni bir suç türü olan “Siber Suç” kavramını çıkarmıştır. Siber suç kavramı ise üst düzey bilgisayar ve ağ kullanma bilgisi gerektiren teknolojinin açıklarından faydalanma ve yine aynı teknolojinin hız, üstünlük, sınır aşan ve gizlenme sağlayan özelliklerini kendi çıkarına kullanarak haksız menfaat elde etmek suretiyle iki farklı biçimde vücut bulmaktadır.<sup>86</sup>

Teknolojinin gelişmesi ile birlikte bir taraftan güvenlik tedbirleri arttırılmaya çalışılırken, diğer taraftan da siber suçlar nicelik ve nitelik bakımından artış göstermektedir. Kişisel çıkar elde etmek için başlayan suçlar artık bireysel olmaktan çıkmakta örgütler tarafında desteklenen organize edilmiş gruplara dönüşmektedir. Bunun yanı sıra sadece anlık menfaat değil aynı zamanda ulusal ve uluslararası teknoloji hırsızlığı, casusluk faaliyetleri ve hizmeti engelleme de siber suç kapsamında değerlendirilmektedir. Bu bağlamda hukuki olarak siber suç kavramının genel bir çerçevesini çizmek oldukça zordur. Yine de Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu 1983

---

<sup>86</sup> Murat Güneştaş, v.d., **Siber Terörizm: Motivasyon ve Yöntem, Siber Suçlar: Tehditler, Farkındalık ve Mücadele**, Ed: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başıbüyük, Global Politika ve Strateji Yayınları, 1. Baskı, Ankara 2015, s.85-89.

Paris Toplantısında siber suç *“bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış”* şeklinde tanımlamıştır.<sup>87</sup> Yaklaşık kırk yıldır gündemde olan ve henüz çerçevesi net olarak çizilmemiş olan tüm siber suçların ortak özelliği hepsinin bilgisayar kullanılarak işlenmiş olmasıdır.<sup>88</sup>Bu suç işleme teknikleri<sup>89</sup>:

### **(1) Bilgi ve Veri Aldatmacası (Data Diddling)**

Bu suç türü, veri sistemlerine girdi yapılırken, kasıtlı olarak hatalı verilerin girilmesi veya veri giriş işlemi yapıldıktan sonra verilerin değiştirilmesidir. Siber suç kapsamında en fazla tercih edilen, gizlenebilir ve kullanım alanı yaygın bir suç tekniğidir.

### **(2) Salam Tekniği (Salami Techniques)**

Bu teknik çok büyük miktarda hesaplardan eksikliği fark edilmeyecek kadar küçük miktarların çalınmasıdır. Genellikle bankalarda görülmektedir ve Truva Atı benzeri yazılımlar kullanılmaktadır.

### **(3) Süper Darbe (Super Zapping)**

Bu teknik, bilişim sistemlerinin çeşitli nedenlerle çalışmaz hale geldiğinde, sistemin tekrar hazır hale geleceği süre zarfında tüm güvenlik önlemlerinin devre dışı olduğu anda uygulanmaktadır.

---

<sup>87</sup> Çakmak ve Demir, **a.g.e.**, s.32.

<sup>88</sup> R.D.Clifford, *Cybercrime*, Carolina Academic Press, Durham, 312s.

<sup>89</sup> Hüseyin Çakır ve Mehmet Serkan Kılıç, **Güncel Tehdit: Siber Suçlar**, Seçkin Yayınevi, 1. Baskı, Ankara 2014, s.22-37.

#### **(4) Eşzamansız Saldırılar (Asynchronous Attacks)**

Herhangi iki işlem arasında, sırada bekleyen işlem üzerinde kötü niyetli değişiklik yapma saldırısıdır.

#### **(5) Truva Atı (Casus Yazılımlar)**

Kullanıcıdan habersiz arka planda işlem yapan programların genel adıdır. Bu yazılımlar virüs etkinliğinde olmayıp bilgisayar internete bağlıyken dışarı veri aktarımı yaparlar.

#### **(6) Zararlı Yazılımlar (Malicious Software)**

Bu yazılımlar bilgisayara zarar veren, bilgi çalan ve virüs etkinliğinde ağda bulunan diğer bilgisayarlarada yayılan yazılımlardır.

#### **(7) Mantık Bombaları (Logic Bombs)**

Önceden belirlenmiş bir tarih geldiğinde veya bir işlem uygulandığında aktif hale gelen virüs programlarıdır. Truva Atı yazılımından tek farkı işleme geçtiğinde saklanmamasıdır.

#### **(8) Oltaya Gelme (Phishing)**

Teknoloji ve sosyal mühendislik bilgileri kullanılarak kişilerin banka hesapları, kredi kartı bilgileri, mahrem verileri kişiyi aldatarak almaktır.

#### **(9) Tarama (Scanning)**

Bu programlar suç işleyen kişiler tarafından sıralı bir dizi işlemle değişen verileri elde etme, raporlama, şifre çözme işlemleridir. Aynı zamanda sistem açıklarını tespit edip güvenliği artırma amacı ile de kullanılabilir.

**(10) Bukalemun (Chamelon)**

Aldatma ve hile programıdır. Kullanıcı adı ve şifreleri taklit ederek gizli verilere ulaşır ve kendisi gizli bir dosya açarak elde ettiği verileri orada saklar.

**(11) İstem Dışı Alınan Elektronik Postalar (Spam)**

Aynı mesajın internet üzerinde çok sayıda kopyasının herkese zorlayıcı nitelikte gönderilmesidir.

**(12) Çöpe Dalma / Atık Toplama (Scavenging)**

Bu teknik bilgisayarda daha önce silinmiş olmasına rağmen izi kalan verilerden ve tam olarak imha edilmemiş kâğıtlardan önemli bilgileri elde etmede kullanılmaktadır.

**(13) Gizli Kapılar (Trap Doors)**

Bu teknikte yazılımı yapan kötü niyetli kişilerin kendileri için programa yerleştirdiği virüs sayesinde sisteme sızmaktadır.

**(14) Sırtlama (PiggyBacking)**

Bu teknik, elektronik veya fiziksel yöntemlerle sistemlere yetkisiz olarak girme çalışmasıdır.

**(15) Yerine Geçme (Masquerading)**

Farklı seviyede yetkilere sahip olan bireylerin olduğu sistemlerde yetkilinin kullanıcı bilgileri ve şifresini kullanılarak sisteme girilmesidir.

### **(16) Sistem Güvenliğinin Kırılıp İçeri Sızılması (Hacking)**

Bu teknikte, kişi veya örgütler kurum veya kuruluşlara ait programlarda varolan açıkları bularak sistemi ele geçirmektedir.

### **(17) Hukuka Aykırı İçerik Sunulması**

İrkçı, ayrımcı, pornografik ve şiddet gibi suç unsurlarının sosyal medyada paylaşılması veya paylaşma tehdidiyle şantaj yapılmasıdır.

### **(18) Web Sayfası Hırsızlığı**

DNS sunucularında hukuka aykırı değişiklik yapma yoluyla bir web sitesine girmek isteyen kişileri yanıltarak farklı bir adrese yönlendirilmesidir.

### **(19) Sosyal Mühendislik**

Bu teknik insan ilişkileri ve insani zaafılardan faydalanarak kurum ve kuruluşlar hakkında bilgi toplamaktır.

#### **b. Siber Saldırı**

Siber suçlar gibi siber saldırılar da gün geçtikçe farklılık göstermekle birlikte bireysel çıkarlar amacıyla tek bir kişi tarafından yapılabileceği gibi, belirli örgütler ve hatta devlet organları tarafından da yapılabilmektedir. Bu bağlamda siber saldırı nedenleri:<sup>90</sup>

\* Siyasi ve politik, ekonomik, dini, ego ve intikam alma gibi sebepler,

\* Saldırı amaçlı ideoloji empoze etme,

---

<sup>90</sup> Telestemur, a.g.e., s.287-288.

- \* Hedef sistemi çökertmek veya bilgi / teknoloji hırsızlığı yapmaktır.

Yukarıda sıralanan nedenler ışığında siber saldırılar özellikle karşı tarafa ait kritik altyapıların otomasyonunu sağlayan bilişim sistemlerini hedef almakta ve kamu düzeninin olumsuz etkilenmesine neden olmaktadır. 2007 yılında Estonya ve 2010 yılındaki İran’da yaşanan StuxNet saldırısında da görüldüğü üzere siber saldırılar toplumda korku, panik huzursuzluk yaratmaktadır.<sup>91</sup> Dolayısı ile internet yardımı ile topluma korku vermek ve ideolojisini zorla kabul ettirmek isteyen terör grupları için siber saldırılar biçilmiş kaftan olmaktadır.

Her ülkede kendini siber saldırılara adanmış gruplar vardır. Örneğin, Türkiye’de Red Hackers Association (R.H.A.) kısa adıyla Redhack grubu saldırılarını sürdürmektedir. Resim 10’da tanıtım afişi gösterilen grubun hedefi, ilgi alanı, etki alanı ve misyonu “*eylemlerine yön verecek esas merkez Türkiye olup; esas görevi, Türkiye Devrimci Hareketi’ne devrimin bilişim alanında, yardımcı olabilmek, Türkiye ve dünya proletaryasına ve ezilen halklara bir nebze olsun dayanışma gösterebilmek*” şeklinde belirtilmekte olup yaptığı bazı saldırılar Tablo 5’te gösterilmektedir.<sup>92</sup>

---

<sup>91</sup> Güneştaş vd., **a.g.e.**, s.92.

<sup>92</sup> Yiğit Turak, Redhack Özelinde Siber Olaylar ve Siber Suçlar, **Yayınlanmamış yayın**, s.9-11.





**Resim 10** – Red Hackers Association (RedHack)’in Tanıtım Afışı<sup>93</sup>

Tarih	Saldırı Şekli	Olay
27.02.2012	Web Sitesi Hackleme	Ankara Emniyet Müdürlüğü internet sitesine saldırılmış ve elde edilen veriler yayınlanmıştır.
20.04.2012	Web Sitesi Hackleme	İç İşleri Bakanlığı sitesine ait bir sayfaya mesaj bırakılmıştır.
27.04.2012	DDos Atak	İnternet servis sağlayıcılarında TTNET’in yaklaşık 2 saat süre ile internet hizmeti aksamıştır.
14.05.2012	Web Sitesi Hackleme	Aile ve Sosyal Politikalar Bakanlığı’nın internet sitesi hacklenmiş ve ana sayfaya bildiri konulmuştur.
29.05.2012	DDoS Atak	THY’nin internet sitesine greve destek amacıyla siber saldırı gerçekleştirilmiştir.
03.07.2012	Web Sitesi Hackleme	Dışişleri Bakanlığı’nın dosya paylaşım sitesine saldırılmıştır.
07.12.2012	Web Sitesi Hackleme	Maliye Bakanlığı internet sitesine saldırılmıştır.
08.01.2013	Web Sitesi Hackleme	YÖK’ün internet sitesine saldırılmış ve elde edilen belgeler yayınlanmıştır.
05.05.2013	Web Sitesi Hackleme	İstanbul Valiliği internet sitesine saldırılmıştır.
11.05.2013	Ddos Atak	Hatay Valiliği’nin sitesi bir gün süre ile erişime engellenmiştir.
31.05.2013	Web Sitesi Hackleme	Gaziantep Büyükşehir Belediyesi internet sitesine saldırılmıştır
28.06.13	Web Sitesi Hackleme	İstanbul İl Özel İdaresi internet sitesine saldırılmıştır
02.07.2013	Ddos Atak	Sivas İl Özel İdaresi’nin internet sitesine saldırılmış ve bir süre erişim engellenmiştir.
14.08.2013	Web Sitesi Hackleme	Ankara ve Adana Büyükşehir Belediyesi Su ve Kanalizasyon İdaresi internet sitesine saldırılmıştır.
14.10.2013	Web Sitesi Hackleme	Türkiye Kamu İşletmeleri Birliği internet sitesine saldırılmıştır ve sayfaya mesaj bırakılmıştır.
10.01.2014	Web Sitesi Hackleme	TBMM’in internet sitesine saldırılmıştır.

**Tablo 5** – RedHack’in Yaptığı Saldırıları ve Olayları

<sup>93</sup>[www.hurriyet.com.tr/amp/gundem/redhack-dsislerinin-belgelerini-yayimlad-21304300](http://www.hurriyet.com.tr/amp/gundem/redhack-dsislerinin-belgelerini-yayimlad-21304300)  
(Erişim Tarihi: 08.11.2020).

### c. Siber Terör

Siberterörizm, basitçe, siber uzayda bilgi işlem kaynaklarını kullanırken başkalarını politik bir amaç için zorlamak şeklinde tanımlanabilmektedir. Genel anlamda ise siberterörizm, terörizm ve siber uzayın yakınsamasını ifade etmektedir. Genel olarak, “*bir devletin hükümetini veya halkını siyasi ve sosyal hedeflere ulaşmak için sindirmek veya zorlamak için yapıldığında bilgisayarlar, ağlara ve burada depolanan bilgilere yönelik yasadışı saldırılar ve saldırı tehditleri*” anlamına geldiği anlaşılmaktadır.<sup>94</sup> 2002'de NIIPC'nin Direktörü Ron Dick'e göre ise siber terörizm, “*bir hükümeti politikalarını değiştirmeye zorlamak amacıyla bilgisayar aracılığıyla şiddet, ölüm ve / veya yıkıma neden olan ve terör yaratan herhangi bir suç eylemi*” anlamına gelmektedir.<sup>95</sup> Wilson oldukça geniş çerçeveden bakarak siber terörizmi, bir izleyiciyi etkilemek veya bir hükümetin politikalarını değiştirmesine neden olmak için, bilgisayarların politik olarak motive edilmiş silah olarak veya alt-ulusal gruplar veya gizli ajanlar tarafından hedef olarak kullanılması şeklinde tanımlamıştır.<sup>96</sup> Pollit, benzer şekilde, çalışmasında siber terörizm terimini “*bilgi, bilgisayar sistemleri, bilgisayar programları ve savaşmayanlara ve hedeflere yönelik şiddete neden olan verilere yönelik olarak alt ulusal gruplar veya gizli ajanlar tarafından önceden planlanmış, politik*

<sup>94</sup> Dorothy E. Denning, Cyberterrorism, **Global Dialogue**, 24 Ağustos 2000, s.1.

<sup>95</sup> Scott Berinato, Cybersecurity-The Truth About Cyberterrorism, CIO From IDG, 15 Mart 2020. [www.cio.com/article/2440933/cybersecurity---the-truth-about-cyberterrorism.html](http://www.cio.com/article/2440933/cybersecurity---the-truth-about-cyberterrorism.html)  
(Erişim Tarihi: 26.10.2020).

<sup>96</sup> Clay Wilson, “Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”, **Congressional Research Service The Library of Congress**, s.4-5.

olarak motive edilmiş saldırılar” şeklinde tanımlamıştır.<sup>97</sup> Bu tanıma göre Pollit, kredi kartı bilgilerini çalmak, pornografik içerikli e-postalar göndermek veya bir web sitesini hacklemek dahil olmak üzere siber suç faaliyetlerini hariç tutmaktadır. Bu alandaki bazı araştırmacılar, bir eylemi yalnızca eylemin yıkım, ölüm ve / veya yaralanmaya neden olması ve halk arasında korku yaratması durumunda siber terörizm olarak nitelendirmektedir.<sup>98</sup> Ayrıca bazıları siber terörizmin yıkıcı yönüne henüz tanık olmadığımızı iddia etmekte ve bu nedenle siber terörizmin hiç var olmadığını bu yüzden öne sürmektedirler.<sup>99</sup> Bu tanımlardan hareketle siber terör ile klasik terör arasındaki farklar Tablo 6’da gösterilmiştir.

	<b>Klasik Terör</b>	<b>Siber Terör</b>
<b>Kullanılan Araç</b>	Silah, Bomba gibi araçlar.	Çipler, bilgisayarlar veya bilgi sistemlerinde kullanılan diğer donanımlar, yazılımlar.
<b>Amaç</b>	Siyasal rejime ve topluma mesaj vermek için terörizmi bir araç olarak kullanmaktır.	Yapılan eylemler ile topluma veya devlete zarar verme, siyasi ve sosyal olarak etkilemek için terörizm bir amaçtır.
<b>Etki Alanı</b>	Saldırının yapıldığı bölge ya da alan ile sınırlıdır.	Ulusal veya uluslararası boyutlarda etkilidir.
<b>Karşılaşılan Risk</b>	Eylemi gerçekleştiren kişi ya da grup yaşamsal risk altındadır.	Herhangi yaşamsal risk olmadan etkili saldırıdır
<b>Denetim</b>	Terörü kontrol altında tutmak, izlemek ve yok etmek kısmi anlamda mümkündür.	Siber teröristleri tespit etmek veya yok etmek imkânsızdır.
<b>Uygulanacak Ceza</b>	Suçun niteliğine göre uygulanacak ceza bellidir.	Suçun niteliğine göre uygulanacak ceza bellidir.

**Tablo 6 – Klasik Terör ile Siber Terör Arasındaki Farklar<sup>100</sup>**

<sup>97</sup> Mark M. Pollitt, “Cyberterrorism: Fact or Fancy?” **Proceedings of the 20th National Information Systems Security Conference**, October 1997, s. 285–289.

<sup>98</sup> Denning, *Cyberterrorism*, s.1-3.

<sup>99</sup> Dorothy E. Denning ve William E. Baugh, Jr., *Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism*, **National Strategy Informatin Center’s Working Group on Organized Crime (WGOC)**, 1997.

<sup>100</sup> Bayraktar, *a.g.e.*, s.78.

Bilişim sistemlerine yapılan saldırılar pasif ve aktif saldırılar olmak üzere ikiye ayrılmaktadır.

### **(1) Pasif Saldırılar**

Bu tür saldırılarda saldırgan bilgi toplamak amacı ile hedef sisteme müdahale etmeden gizliliği ihlal etmektedir.

### **(2) Aktif Saldırılar**

Bu tür saldırılarda saldırgan hedef sistemin en önemli özelliği olan sürekliliğini ve çalışırılığını kesintiye uğratarak sistemin tutarlılığını veya doğrulama mekanizmalarını aşmakta ve bunu hedef sistemin işleyişine müdahale ederek gerçekleştirmektedir.

### **(3) Aktif ve Pasif Saldırıların Kullanımı**

Devlet ve askeri sistemlerde en önemli olgu gizlilikdir. Gizlilik ise terör grupları tarafından hem pasif hem de aktif saldırı yöntemleri ile ihlal edilmektedir. Ancak saldırganlar her ne kadar izlerini örtme çabası içerisinde olsalar da yeterince başarılı olamazlar. Çünkü saldırganın bir şekilde eriştiği sistemin nerede ve nasıl kayıtlar tuttuğunu tam olarak bilmesi imkânsızdır.

Teröristler ağ protokollerini, sunucuları, web sayfalarını, sosyal medya ve benzeri teknolojilerle sanal dünyayı.<sup>101</sup>

\* İnternetin çok büyük kitlelere ulaşım imkânı vermesinden dolayı propaganda aracı olarak,

---

<sup>101</sup> Güneştaş vd., a.g.e., s.97.

- \* Asılsız veya abartılı haberler yayma yoluyla halkı korkutma, sindirme aracı olarak,
- \* Sosyal medyadan kişilerin bilgilerine ulaşılabilirdiği için eleman temin aracı olarak,
- \* Bilişim sisteminin sağladığı gizlilik özelliği ile iletişim ve örgüt yönetim aracı olarak,
- \* Uzaktan erişim imkânı sayesinde eğitim aracı olarak,
- \* Terörist eylemleri gerçekleştirebilmek için gelir kaynağı aracı olarak kullanılmaktadır.

Teröristler, internet ortamında diğer eylem alanlarına kıyasla eş benzeri görülmemiş avantajlar elde etmektedir. Bu avantajlar:<sup>102</sup>

- \* Daha az parasal kaynak ve üye ihtiyacı gerektirir,
- \* Planlama ve eylem konvansiyonel terörist eylemlerine kıyasla daha kolaydır.
- \* Eylem için sahip olunan bilişim sistemlerinin çok teknolojik olması gerekmez.
- \* Eylemden önce, eylem esnasında ve sonrasında tespit edilme ve özellikle kimliklerin açığa çıkması oldukça güçtür.
- \* Muhtemel hedef olarak seçilen yerlerin miktarı ve çeşidi çok fazladır.

---

<sup>102</sup> Sertaç, H. Başeren, “Terrorism with Its Differentiating Aspects”, **Defence Against Terrorism Review**, Cilt: 12, Sayı: 1, Bahar 2008, s.2-4.

- \* Eylem için hedef bölgeye gidilmeye gerek yoktur. Çok uzak noktadan gerçekleştirilebilir.
- \* Medyada daha fazla yer bularak eylemlerinin etkilerini daha uzun süre hissettirebilirler.
- \* Medya aracılığı ile daha fazla kişiye ulaşarak toplumun büyük bir kesimini etki altına alıp, propagandalarını gerçekleştirebilirler.

Siber terör eylemleri genel olarak şiddet içeren ve şiddet içermeyen eylemler olarak sınıflandırılmaktadır.<sup>103</sup> Şiddet içermeyen eylemler, terör örgütlerinin eylemlerini hayata geçirmek için bilişim sistemlerinden faydalandıkları propaganda, eğitim, haberleşme ağlarına ve maddi kazanımlara yönelik girişimlerdir. Şiddet içeren eylemler ise propaganda ağırlıklı olmanın yanı sıra devletlerin ve toplumların varlıklarını sürdürmelerine hayati seviyede engel olmayı amaç edinen fiili saldırılar olarak tanımlanabilir. Bu bağlamda genel olarak değerlendirildiğinde siber terör, bir yandan şiddet içeren faaliyetler ile toplumları tehdit eden bir olgu olarak tanımlanırken, diğer yandan bu eylemlerin sonucu olarak toplumsal krizlere yol açarak devlet otoritesine balta vuran siyasal sonuçlar doğurmaktadır.

Siber terör eylemleri şiddet içerip içermediklerine bakılmasızın hedef aldıkları bilgi sistemlerine zarar vermede ihtiyaç duyduğu teknoloji kullanma yeteneğine, bu hedeflerin zayıf noktalarını belirlemede ihtiyaç duyduğu hedef analiz düzeyine ve bunları gerçekleştirmede ihtiyaç duyduğu örgütsel kapasite seviyesi olmak üzere üç düzeye

---

<sup>103</sup> Bayraktar, a.g.e., s.78-79

ayrılmaktadır.<sup>104</sup> Buna ek olarak Denning’de terör örgütlerini bu üç özelliği sağlama derecelerine göre; “basit-yapılandırılmış”, “ileri düzeyde-yapılandırılmış” ve “karmaşık koordinasyonlu” olmak üzere üç farklı seviyede ele almıştır.<sup>105</sup> Bu iki çalışma bir bütün halinde Tablo 7’de gösterilmektedir.

Siber Terör Düzeyleri	Hedef	Hedef Analizi	Örgütsel Kapasite	Etki Kontrolü	Potansiyel Fayda
<b>Basit-Yapılandırılmamış</b>	Tek sistem ya da ağ	Başlangıç Seviyesinde	Az Seviyede	Odaklı Değil	Propaganda
<b>İleri Düzeyde-Yapılandırılmış</b>	Birden çok sistem ya da ağ	Orta Seviyede	Orta Seviyede	Odaklı	Taktiksel Eylemler (Gösteri amaçlı ya da konvansiyonel eylemler destek)
<b>Karmaşık-Koordinasyonlu</b>	Birden çok ağ	Detaylı	Çok İleri Düzeyde	Kontrol Edilebilir	Stratejik Eylemler

**Tablo 7 – Siber Terör Eylem Düzeyleri**

Sonuç olarak günümüzün ve geleceğin terör grupları gerçek dünyadaki eylemlerini sanal dünyaya taşımaktadırlar. Çünkü Denning’in de kitabında bahsettiği üzere geleceğin teröristi bilgisayar klavyesi ile büyük bir bombanın oluşturacağı patlamadan daha fazla etki yaratacaktır.<sup>106</sup> Günümüzde ise siber teröristlerin her ne kadar bilgi altyapılarına ve diğer iletişim ağlarına saldırmayı düşündüğünü gösteren kanıtlar olsa da neden tam olarak algılanamadığına dair en iyi

<sup>104</sup> Hikmet Topal, **Siber Terör**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul 2004, s.32-34.

<sup>105</sup> Denning, *Cyberterrorism*, s.8.

<sup>106</sup> Dorothy Denning, , **Information Warfare and Security**, Addison Wesley, 1. Baskı, New York, 1999, s.70.

açıklama Brenner ve Goodman'ın, uluslararası teröristlerin teknik altyapı açısından yeteneklerinin olmadığı şeklindeki yorumudur.<sup>107</sup> Bu açıklamaya göre batı özellikle batı toplumu kendini güvende hissederek rutin hayatlarına devam etmektedirler. Ancak, Brenner ve Goodman bu teori ile ilgili olarak teröristlerin aktif olduğu ülkelerin diğer ülkelerin bilgi altyapısına karşı siber saldırılar başlatmak için gerekli olan gelişmişliğe sahip olduğu gerçeğini göz ardı etmektedirler. Çünkü, örneğin, Pakistanlı hacker grupları, G-Force Pakistan ve The Pakistani Hackers Club ve teröristlerin, örgüte sağladıkları finansman ile siber saldırılar başlatacak uzmanlığa ve motivasyona sahip hacker paralı askerleri istihdam etme olasılığı oldukça yüksek ihtimaldir. Bunun yanı sıra bu terör eylemlerini gerçekleştiren örgütlerin finansman kaynağı olarak bir devlet tarafından desteklenmesi halinde ise oluşan siber suç kavramı daha geniş bir alana yani siber savaşa evirilmektedir.

#### ç. Siber Savaş

Toplumsal yapıya bakıldığında taşları yontup silah olarak kullanan Avcı Toplayıcı Toplumdan mekanik ve elektronik savaş teçhizatlarının kullanıldığı Sanayi Toplumuna gelinmiştir. Süper Akıllı Toplum döneminin yaşandığı bu günlerde ise Bilgi Toplumu'nun savaş yaklaşımına geçilmiştir. Bilgisayarların ve sanal ağların gelişmesi ile siber uzayda tutulan, ekonomik ve stratejik değeri yüksek taşınabilir ve işlenebilir veriler hedef alınmaktadır. Bu

---

<sup>107</sup> Susan W. Brenner ve Marc D. Goodman, In Defence of Cyberterrorism: An Argument for Anticipating Cyber-Attacks, **Journal of Law, Technology and Policy**, Cilt:1, 2002, s.1-57.



bağlamda bilişim teknolojilerinin gelişiminin savaş kavramını ve çerçevesini değiştirdiği görülmektedir. Bilginin daha da çok değerlendirildiği Bilgi Toplumu'nda devletler konvansiyonel savaşlar yerine işletmeler, dini gruplar, siber teröristler, uyuşturucu kaçakçıları ve bilişim korsanları gibi örtülü unsurlar ile Bilgi Savaşları'na başlamıştır. Bunun en güzel göstergesi Emekli Orgeneral Hilmi Özkök'ün “*İnternet korkakların platformudur. Demir çıktı mertlik bozuldu; telli demir çıktı artık her şey bozuldu*” sözleridir.<sup>108</sup>

Siber Savaş “*hükümetlere bağlı veya hükümet oluşturmaya istekli meşru organize gruplar arasındaki büyük ölçekli şiddetli çatışma durumu*” olarak tanımlanmaktadır.<sup>109</sup> Bu bağlamda, tanımdan da görüldüğü üzere siber savaş, kişisel menfaat sağlama suçundan ve ideolojilerini yayma ve siyasi amaç hedefiyle yapılan siber terörden farklılık göstermektedir. Dolayısı ile siber suç ile siber terör ayrımı çok muğlakken, siber savaş kavramı diğerleri gibi interneti kullanarak yapılsa da saldırılar bir devlet ya da örgütlenmiş bir otorite tarafından gerçekleştirilmekte olup motivasyon ve amaçsal düzeyde daha koordineli ve daha yoğun bir baskı ile düzenlenmektedir.<sup>110</sup>

Diğer bir açıdan siber savaş kavramı siber teknolojilerinin askeri kullanımı olarak tanımlanabilmektedir. Amerikan Ulusal Güvenlik Dairesi (NASA) eski başkan yardımcısı Mike McConnell'in 2003 yılı

<sup>108</sup> Hürriyet Haber: “Sezer:Türkiye'nin Lübnan'a asker göndermesine karşıyım”, 25.08.2006, [www.hurriyet.com.tr/gundem/4980763.asp?m=1](http://www.hurriyet.com.tr/gundem/4980763.asp?m=1) (Erişim Tarihi 07.11.2020).

<sup>109</sup> Haldun Yalçınkaya, **Savaş: Uluslararası İlişkilerde Güç Kullanımı**, İmge Kitabevi, Ankara 2008, s.40.

<sup>110</sup> Çakmak ve Demir, **a.g.e.**, s.32.

Nisan ayında söylediği ‘30 bilişim korsanı ve 10 milyon dolar, Amerika Birleşik Devletleri’ni (ABD) dizleri üstüne çökertebilir’’ sözü her şeyi özetler niteliktedir.<sup>111</sup>

Siber savaşta hedef bilgi işlem alt yapısıdır. Siber savaş kapsamında bir tarafın elde ettiği yüksek değere sahip askeri veya sivil sırların açıklanması ve bilişim teknolojilerinin ele geçirilmesi ülkeye küresel çapta zarar verebilmektedir. Örneğin, hiç elektrik kesintisi yaşamamış toplumlar karanlığa gömülebilir, haberleşme ağının kesilmesi nedeniyle habersiz kalabilir, sivil hava araçları aniden uçuşa yasak alanlara girebilir veya havada çarpışabilirler. İngiliz Times Gazetesinde çıkan ‘İsrail siber askerler tarafından destekleniyor’’ haber başlığı İsrail – Lübnan savaşının siber uzaya taşındığını göstermektedir.<sup>112</sup> Buna ek olarak Can Dündar 2006 yılında yazdığı yazıda örnekler sunarak siber savaşın gelişimini göstermektedir. Can Dündar’a göre:<sup>113</sup>

- \* 2. Dünya Savaşı’na radyo damga vurmuştur.
- \* Vietnam savaşında televizyon silaha dönüşmüştür.
- \* Amerika Vietnam Savaşı’nı oturma odalarında kaybetmiştir.
- \* Savaş yayını tekelleşmiş ve kontrol altına alınmıştır. Yanlı yayınlar başlamıştır.
- \* Youtube, İsrail- Lübnan Savaşı’nın kayıtlarını sunmuştur.

<sup>111</sup> [www.theage.com.au/articles/2003/04/07/104567622561.html](http://www.theage.com.au/articles/2003/04/07/104567622561.html) (Erişim Tarihi 11.10.2020).

<sup>112</sup> [www.timesonline.co.uk/article/0,,3-2289232,00.html](http://www.timesonline.co.uk/article/0,,3-2289232,00.html) (Erişim Tarihi 11.10.2020).

<sup>113</sup> Can Dündar, ‘‘Savaş şimdi de İnternette’’, **Milliyet**, 22.07.2006  
[www.milliyet.com.tr/2006/07/22/yazar/dundar.html](http://www.milliyet.com.tr/2006/07/22/yazar/dundar.html) (Erişim Tarihi 11.10.2020).

\* İnternet sayesinde söz hakkı devlet büyüklerinden sıradan insanlara geçmiştir.

Siber savaş bilgi savaşı olarak ta adlandırılmaktadır. Bilgi savaşı “*bir buhran ve çatışma sırasında bilgi veya bilgi teknolojilerinin belirli bir hasmun veya hasımlara yönelik belirli gayelerin başarılması veya ilerletilmesi amacıyla kullanılması*” şeklinde tanımlanabilir.<sup>114</sup> Bazı kaynaklarda ise bilgi savaşı siber savaştan çok daha kapsamlıdır. Örneğin Taylor vd. bilgi savaşı ile siber terörizm arasındaki farkı açıklığa kavuşturmak için siber terörizmin bilgi savaşının bir bileşeni olabileceğini, başka bir deyişle bilgi savaşının siber terörizmi kapsadığını dile getirmiştir.<sup>115</sup>

### 3. Dünya’dan Siber Terör Örnekleri

1960’lı yılların başından itibaren bilgisayar kullanımının yaygınlaşması ve internet temellerinin atılması ile gelişim göstermeye başlayan bilişim teknolojileri ilerlemenin yanı sıra diğer ülke sistemlerinin çalışmasını önleyecek yönde de gelişme göstermiştir.<sup>116</sup>Bu önleme yöntemlerinin başlıca amaçları: Ekonomik yönde avantaj sağlamak, siyasi talepleri dikte etmek, saldırı ve zarar verebilme gücünü ispat etmek, veri ve teknoloji hırsızlığı yapmak,

<sup>114</sup> Gürol Canbek ve Şeref Sağıroğlu, **Bilgi ve Bilgisayar Güvenliği:Casus Yazılımlar ve Korunma Yöntemleri**, Sayfa Uygulama Baskı ve Cilt, Birinci Baskı, Ankara 2006, s.143.

<sup>115</sup> Süleyman Özeren, Cyberterrorism and International Cooperation:General Overview of the Available Mechanisms to Facilitate an Overwhelming Tasks, **Responses to Cyber Terrorism**, (Edited by Centre of Excellence Defence Against Terrorism, Ankara Turkey), **IOS Press**, Amsterdam, 4-5 October 2007, s.71.

<sup>116</sup> Hasan Çiftci, **Her Yönüyle Siber Savaş**, Tübitak Popüler Bilim Kitapları, 1. Baskı, Ankara 2013, s.163.

diğer unsurun hizmet vermesini engellemek, askeri üstünlük sağlamak, propaganda yapmak veya sadece eğlenerek karşı unsuru küçük düşürmek olabileceği değerlendirilmektedir. Ancak geçmişte yaşanan saldırılar incelendiğinde, siber saldırının gerçekleştirildiği sistemlerin zayıf tarafları yanında kullanıcı hatalarından da istifade edildiği değerlendirilmektedir.

### **a. Çin Büyükelçiliğinin Bombalanması**

1999 yılının mayıs ayında, NATO jetlerinin yanlışlıkla Belgrad'daki Çin Büyükelçiliğini bombalaması üzerine Çin Kızıl Korsanlar Birliği ABD web sitelerine saldırılar düzenlemiştir.<sup>117</sup>

### **b. Hainan Adası Olayı**

1 Nisan 2011 tarihinde bir Çin jeti ile ABD casus uçağının havada çarpışması sonucunda Çin jeti düşmüş; ABD uçağı ise Hainan Adası'na mecburi iniş yapmaya zorlanmıştır. Bu olay üzerine 80000'den fazla bilgisayar korsanı ABD'ye karşı savunma harekâtı başlatmıştır. The New York gazetesi tarafından yayınlanan bu olay “*World Wide Web War I*” olarak isimlendirilmiştir.<sup>118</sup>

### **c. Estonya**

2007 yılında Estonya Hükümeti'nin Rusların Estonyalıları Nazi işgalinden kurtarmasını simgeleyen Kızıl Ordu Anıtı'nı kaldırması

<sup>117</sup> Polatkan Akdağ, **Siber Suçlar ve Türkiye'nin Ulusal Politikası**, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara 2009. s.93.

<sup>118</sup> Craig S. Smith, “May 6-12; The First World, Hacker War”, **The New York Times**, 13 Mayıs 2001. www.nytimes.com, (Erişim Tarihi:08.11.2020).

üzerine Rusya'daki amatör kullanıcılar dâhil bir ay boyunca Estonya İnternet altyapısına siber saldırılar gerçekleştirmişlerdir.<sup>119</sup>

#### **ç. ABD Gizli Askeri Ağında USB Olayı**

2008 yılında yaşanan bu olayda, yüklenici firma personeli ABD askeri bilgisayarına virüslü usb bellek takmış ve bu nedenle ABD'nin tasnif dışı ve gizli gizlilik dereceli ağları etkilenmiştir.<sup>120</sup> Bu olayın ABD Siber Komutanlığı'nın kurulmasının gerekçesi olduğu iddia edilmektedir.

#### **d. Gürcistan**

2008 yılında, Rus bilgisayar korsanları Gürcistan devletine ait resmî web sitelerine saldırarak internet alt yapısını çökertmişlerdir. Gürcistan, siber saldırıları durdurabilmek için Rusya'dan gelen İnternet trafiğini bloke etmiş; ancak, korsanlar saldırılarına Çin, Kanada, Türkiye ve Estonya'da bulunan köle bilgisayarlar üzerinden devam etmiştir.

#### **e. Conficker Solucanı**

Microsoft işletim sistemlerini hedef alan conficker solucanı ilk kez 2008 yılının Kasım ayında fark edilmiştir. Bu solucan işletim sistemi açıklarından faydalanarak bilgisayarı ele geçirmiş ve yedi ila onbeş

---

<sup>119</sup> Ian Taylor, "Russia accused of Unleashing Cyberwar to Disaple Estonia", **The Guardian**, 12 Mayıs 2007. [www.theguardian.com](http://www.theguardian.com) (Erişim Tarihi:08.11.2020).

<sup>120</sup> CNET, "Bad Flash Drive caused Worst U.S. Military Breach", [http://news.cnet.com/8301-27080\\_3-20014732-245.html](http://news.cnet.com/8301-27080_3-20014732-245.html) (Erişim Tarihi: 08.11.2020).

milyon civarında bilgisayara bulaşmıştır.<sup>121</sup> 2003 yılındaki Welchia solucanından sonra gelmiş geçmiş en çok bilgisayara bulaşan ikinci solucan olmuştur.

### **f.Cast Lead Harekâtı**

2008 yılında İsrail Devleti'nin Hamas TV yayınına hekleyerek Hamas liderlerinin öldüğünü gösteren Arapça “Zaman Tüküyor” başlıklı bir çizgi film yayınlaması üzerine Filistinli siber korsanlar İsrail Web sitelerine saldırmış ve binlerce web sitesini değiştirerek İsrail aleyhtarları ilanlar yerleştirmişlerdir.

### **g. Joint Strike Fighter – 35 (JSF-35) Verilerinin Çalınması**

2009 yılında Çin kaynaklı olduğu tespit edilen siber saldırılarla F-35 uçağının tasarımı ve elektronik sistemlerini içeren terabaytlar boyutunda veri çalınmıştır.

### **ğ. Mavi Marmara**

31 Mayıs 2010 tarihinde, abluka altında bulunan Gazze'ye insani yardım götüren ve çoğunluğun Türk gönüllülerden oluştuğu gemilere düzenlenen İsrail saldırısı üzerine Türk bilgisayar korsanları İsrail'in Likud partisinin web sitesine “Ne Mutlu Türküm Diyene” sözleri ile birlikte Türk Bayrağı ve Atatürk'ün fotoğrafını koymuşlardır.

---

<sup>121</sup> Seungwon Shin, ve Guofei Gu, Conficker and Beyond: A Large-Scale Empirical Study, Proceedings-Annual Computer Security Applications Conference, ACSAC, December 2010, s.151.

## h. Stuxnet

2010 yılında bir İran bilgisayarında keşfedilen, İsrail'in desteği ile casusluktan çok İran'daki Natanz Güç Tesislerinde yer alan çok hassas bir endüstriyel ekipman parçası olan santrifüjleri sabote etmek için tasarlandığı değerlendirilen stuxnet solucanı izole bir ağa sahip güç santraline bir USB aracılığı ile girdiği tahmin edilmektedir.<sup>122</sup> Tablo 8'de İran ve diğer ülkelerde etkilenen bilgisayarların yüzdesi verilmiştir.

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

**Tablo 8** – Stuxnet Solucanından Etkilenen Ülkeler ve Etkilenme Yüzdeleri<sup>123</sup>

## 4. Siber Terörizme Karşı Siber Güvenlik Standartları

Kişilerin, işletmelerin, kurum ve kuruluşların ve hatta devletlerin bilişim sistemlerine olan bağımlılıkları arttıkça, siber terörizm faaliyetlerine maruz kalmamak için siber güvenlik sistemlerine olan ihtiyaçları da artmaktadır. Ancak unutulmaması gereken nokta, Siber güvenliğin tek başına bir tedbir olmasından ziyade milli güvenliğin bir parçası olmasıdır.

<sup>122</sup> Marie Baezner ve Patrice Robin, **a.g.e.**, s.4-5.

<sup>123</sup> Çiftci, **a.g.e.**, s.174.

Siber güvenlik tarihine bakıldığında tarihsel süreçte 1970 ve 1980'lere kadar sadece bilgi güvenliği adı altında milli ve askeri iletişim sistemlerinin faaliyetinin devamlılığı amacıyla iletişim güvenliği üzerine odaklanıldığı ve bu yönde bir standartlaşma uygulanmaya çalışıldığı görülmektedir.

Standartlar kavramı, aynı faaliyetin aynı şekil ve süreçte yapılmasını sağlamaya çalışan işlemler düzenidir. Bu nedenle standartları oluşturmadan önce bilgiyi güvence altına almayı ve bu faaliyeti destekleyen kavramların belirlenmesi gerekmektedir.

#### a. Bilgi Güvencesi

Elde edilen verinin belli bir anlam ifade edecek şekilde düzenlenmiş halide bilgi denilmektedir. Bu bağlamda bilgi elde edilen verilerin mantığa uygun bir şekilde dönüştürülmesi, varsayımlarla desteklenmesi, formül ve ilişkilerle bağdaştırılması veya tamamen basitleştirme gibi bir dizi işlemlere maruz kalabilmektedir. Bilginin güç olduğunun fark edilmesi ile birlikte bilgi teknolojilerine olan yatırımlar arttırılmış dolayısı ile savaş platformu da bu yöne doğru kaymıştır. Hatta ortaya çıkan bilgi savaşı milli devletlerin ordularının dışına sıçramış ve işletmeleri, dini grupları, terörist örgütleri, uyuşturucu kaçakçıları, internet korsanlarını da kapsamına almıştır. Yeni kişi ve grupların eklenmesi ile etki alanı genişleyen bilgi savaşları saldırı, böl, parçala, yönet ve elde et işlemlerinden ziyade bir üst kavram olarak siber savaşı da içerisine almaktadır.<sup>124</sup>

---

<sup>124</sup> Görol Canberk ve Şeref Sağıroğlu, **Bilgi ve Bilgi Güvenliği Casusu Yazılımlar ve Korunma Yöntemleri**, Grafiker Ltd.Şti, 1. Baskı, Ankara 2006, s.145-146.



### (1) Bilgi Güvencesi Temel Unsurları

Bilgi güvenliğinin Siber güvenliği içine alması gibi bilgi güvencesi de bilgi güvenliğini içine almaktadır. Bu bağlamda bilgi güvencesi Şekil 6'da gösterildiği üzere beş alt unsurdan oluşmaktadır.



Şekil 6 – Bilgi Güvencesi Unsurları<sup>125</sup>

(a) **Gizlilik:** Bilgiyi, bağlantı varlığını, trafik akışını ve bilgi içeriğini yetkisiz şahıslara karşı koruyan gizlilik unsuru erişim kısıtlaması ile birlikte içeriği güvence altına almaktadır.

(b) **Bütünlük:** Bilginin istemli veya istemsiz olarak yetkisiz karıştırmalara ve değiştirilmesine karşı güvence altına alınmasıdır.

(c) **Kullanılabilirlik:** Kullanıcıların ihtiyaç duydukları anda bilgiye, bilgi servislerine ve bilgi kaynaklarına ulaşabilmesini ve iletişim servislerinin istendiği anda kullanıma hazır halde bulunmasının güvence altına alınmasıdır.

<sup>125</sup> Çiftci, a.g.e., s.220.

(ç) **Kimlik Doğrulama:** Sadece yetkili kişiye bilgiye ulaşabilme ve işlemleri gerçekleştirebilme yetkisinin verilmesini güvence altına alınmasıdır.

(d) **İnkâr Edememe:** Kaynakların ve bilgileri gönderilip alındığının güvence altına alınmasıdır.

## (2) Bilgi Güvencesini Destekleyen Kavramlar

(a) **INFOSEC (INFOrmation SECurity):** Bilgi ve silgi sistemlerini yetkisiz girişlere, verilerin değiştirilmesine ve yetkisiz şahıslar tarafından kullanım dışı bırakılmaya karşı korumaktadır. Kısaca tüm bilgi alt yapısını korumayı içerir.

(b) **COMSEC (COMmunacation SECurity):** Sızıntı Güvenliği, Elektronik Güvenliği, İletim Güvenliği ve Kriptografik Güvenliği adı altında dört bileşeni içeren COMSEC telekomünikasyondan elde edilen bilgilere yetkisiz şahısların erişmesini engellemektedir.

(c) **TEMPEST:** Diğer bileşenlerin aksine bir kısaltma olmayan bu kavramda, elektrikle çalışan teçhizattan ışıma ve iletkenlik yoluyla yayılan bilgilerin korunması amaçlanmaktadır.

(ç) **COMPUSEC (COMPUter SECurity):** Yazılım ve donanım araçlarının tamamını içeren bu kavramda bir bilgisayarda işlenen veya depolanan verilerin güvenliğini, bütünlüğünü, kullanılabilirliğini koruma altına almak hedeflenmektedir.

## b. Temel Güvenlik Standartları

ABD’de Trusted Computer System Evaluation Criteria (TCSEC) ve Avrupa’da Information Technology Security Evaluation Criteria (ITSEC)’ten sonra genel ve özel sektör uygulamalarında kullanılan ürün ve protokoller International Organization for Standardization (ISO) adı altında birleştirilmiştir. Bu bağlamda kullanılan güvenlik standartları Tablo 9’da sunulmuştur.

Adı	Kaynağı	Tarihi	Zorunluluk
COBIT	Uluslararası Kurum: ISACA	1996	Yok
ITIL / BS 15000	Uluslararası	1989	Yok
NIS SP 800-30	ABD: Net	2002	Yok
ISO 13335-2 (ISO 27005)	Guidelines for Management of IT Security	1996	Standart
ISO 15408	Common Criteria	1996	Sertifika
ISO 27001	BS 7799-2’nin yeni hali	2005	Sertifika
ISO 27002	17799 ve BS 7799-1-in yeni hali	2007	Sertifika

**Tablo 9** – Yaygın Güvenlik Standartları<sup>126</sup>

Tablo 9’da gösterilen standartlardan Control Objectives for Information and Related Technology (COBIT), ilk defa 1996 yılında ortaya çıkmış ve işletmelerin bilgi yönetimi ve yönetişim çerçevesinde stratejiler geliştirmelerine, planlamalarına, düzenlemelerine, izlemelerine ve uygulamalarına yardımcı olmayı amaçlamaktadır.<sup>127</sup> Information Technology Infrastructure Library (ITIL) ise 1980’lerin başında İngiliz Hükümeti Merkezi Bilgisayar ve Telekomünikasyon Ajansını (CCTA)’yı görevlendirerek bilgi teknolojisi hizmet yönetimi için çerçeve oluşturma ve bilişim teknoloji servislerini en iyi şekilde

<sup>126</sup> Çiftci, a.g.e., s.224.

<sup>127</sup> www.beyaz.net 25 Mart 2020 (Erişim Tarihi:08.11.2020).

yönetmek üzere geliştirilmiş servis yönetim metodolojisini hayata geçirmiştir.<sup>128</sup>ISO 27001 standardı, kurumlardaki bilgi güvenliği sürecinin değişen güvenlik ihtiyaçlarını yaşayan sistem olarak değerlendirir. Son olarak ISO 27002 Standardı, bilgi güvenliği uygulama sürecinde hayata geçirilebilecek tedbirleri içeren bir önlem havuzudur.

---

<sup>128</sup> Lee Chih Hui, **Information Technology Infrastructure Library (ITIL): An Approach To Optimize Best Practices In It Service Delivery**, Universty of Malaysia, 2012, s.3.

## BEŞİNCİ BÖLÜM

### SİBER TERÖRİZMİN ETKİ ALANLARI

#### 1. Küreselleşmenin – Siber Terör ve Siber Tehdit İlişkisi

Küreselleşme dar anlamda ürünlerin, fikirlerin, kültürlerin ve doğal olarak insanların yaşadıkları ulus devletlerin sınırlarına bağımlı olmaksızın bütünleşmek şeklinde açıklanabilir. Bilişim ve teknoloji çağını yaşadığımız günümüzde küreselleşmenin geçmişte kazandığı ivmeyi arttırdığı yakın çevrede dahi gözlemlenebilen bir durumdur. Teknolojinin gelişiminin yanı sıra ulaşılabilir olması ile küreselleşme internet teknolojisinin yaygınlaşması sayesinde gelişmeye devam etmekte ve insanların kullanmakta olduğu telefon, bilgisayar veya benzeri cihazlarla internet üzerinde çevrimiçi bir hale gelmesiyle anlık iletişimin sağlandığı boyuta ulaşmıştır.

Hemen hemen her şeyin siber uzaya aktarıldığı günümüzde küreselleşmenin yıkıcı etkilerinden etkilenmemek için iletişim ve bilişim altyapılarının korunması önem arz etmektedir. Çünkü internete bağlı her hangi sistem koruma programları ile desteklenmediği sürece dünyanın herhangi bir yerinden yapılacak bir saldırıya karşı savunmasız bırakılmış demektir Bu da siber terörist ve suçlulara avantaj sağlamaktadır. Siber uzayın kullanımı saldırganların yakalanma riskini azaltmakta ve fiziksel olarak verilecek hasarlardan çok daha fazlasını doğrudan veya dolaylı olarak insanların can ve malına saldırmadan elde etmeye imkân vermektedir. Bu bağlamda küreselleşme ile siber terörün toplumda korku ve panik havası yaratmak için öncelikle bilişim ve iletişim alt yapılarını hedef almakta

olduğu, sadece internete bağlı olması şartıyla dünyanın her yerinden gerçekleştirilebileceği, tespit edilmesinin zor olduğu, toplum üzerinde klasik bir bombalama eyleminden çok daha fazla etki yaratan saldırılar olduğu değerlendirilmektedir. Bu saldırılar düşman devletler, teröristler, casuslar, hackerler, ticari rakipler, bilmesi gereken prensibinden daha fazla bilgiye sahip olmuş bilinçsiz personel, ve hatta mutsuz çalışanlar tarafından gerçekleştirilebilmektedir.

## **2. Küreselleşme – Güvenlik ve Terör Örgütleri İlişkisi**

Küreselleşme ile birlikte, terörizm, bilişim ve siber suçlar, insan, yabani hayvan, organ, silah mühimmat ve uyuşturucu madde kaçakçılığı gibi uluslararası güvenliği tehdit eden suçların ulusal iç güvenliğe etkileri de farklı bir boyuta taşımaktadır. Böylece, küresel boyutta ortaya çıkan asimetrik risk, tehlike ve tehditler ülkelerin ulusal ve iç güvenlik politikalarında köklü değişimlere gitmelerine yol açmaktadır. Siber uzayın tüm avantajlarını kullanan terör örgütleri karşısında ulusal güvenlik politikalarının yeterli seviyeye ulaşamaması nedeniyle siber güvenlik kapsamında uluslararası işbirlikleri kurulmaktadır. Bu işbirliklerinde elde edilen kazanımların yanı sıra yaşanan koordinasyon eksikliği, ulusal bilişim teknolojisinde güvenlik zafiyetlerinin bulunması, ülke içindeki etnik ve mezhepsel ayrışmalar gibi durumlar, güvenliğe ilişkin tehdit, tehlike ve risk algılarının da her geçen gün farklılaşmasına neden olmaktadır.

Bu bağlamda küreselleşmenin siber güvenlik ve terör örgütleri ile olan ilişkisinde direkt olarak bağlantı olmasa da küreselleşmenin sağladığı imkânlarla terör örgütlerinin kişilere erişimi kolaylaşmış özellikle

sosyal medya üzerinden ideolojilerini yayma fırsatı bulmuş ve yalan veya taraflı yorumlar içeren paylaşımlarla toplumda korku ve panik havasını hep canlı tutma imkânına kavuşmuştur. Çünkü terör örgütlerinin gündeme getirdiği bir konu iç güvenliğe ilişkin bir sorun olmakta dolayısı ile ulusal ve uluslararası güvenliğe ilişkin yasa ve politikaları da olumsuz etkiyebilmektedir. Aynı şekilde ulusal ve uluslararası güvenlik ile ilgili gelişmeler, iç güvenliğe ilişkin etkiler de meydana getirebilmektedir.

### **3. Terör Örgütleri – Sosyal Medya Kullanımı İlişkisi**

Facebook, Twitter, Instagram ve Whatsapp gibi sosyal medya platformlarının insanların etkileşimi amacıyla sağlamış olduğu sanal dünya toplum için hayatı ve iletişimi kolaylaştırmanın yanı sıra kötü niyetli ve zarar verme amaçlı bir fikir etrafında toplanmış gruplar tarafından da kullanılabilir. Bu bağlamda bu platformların sosyal etkileşim ve alışveriş gibi iyi niyetli kullanımlarının yanında dolandırıcılık, taciz, tehdit, korkutma ve gizli toplantı platformlarına dönüşebildiği açıkça görülmektedir.

Sosyal medya, her ne kadar ulusal ve uluslararası güvenlik kurumlarının gözetimi altında olsa da, kullanıcılar için zorlanmadan veya açığa çıkmadan geniş kitlelere erişimi mümkün kılmaktadır. Gerçek kimlik sunma gibi bir zorunluluğun olmaması, sahte ve trol hesaplar ile toplumun istenildiği şekilde yönlendirilmesine, korku ve paniğe sevk edilmesine imkân vermektedir. Ayrıca bireyler çoğu zaman bilinçli olarak oluşturulan bilgi kirliliğinden etkilenmekte, yalan ve yönlendirilmiş haberleri gerçeklerden ayırt edememekte, kötü

niyetli propagandaya alet olmakta ve kötü niyetli kişilerce kolayca galeyana gelmektedirler. Toplumun bu yalan ve yönlendirilmiş bilgiye kaynağını sorgulanmadan inanması, bilgiyi bilinçsizce daha fazla yayması toplumsal tepkilerin artmasına ve nihayetinde devlet güçlerinin yerel ve genel anlamda aciz gösterilebilmesine neden olmaktadır. Terör örgütleri devlet güçlerinin aciz kaldığı durumları sosyal medyada gerçeğe aykırı şekilde abartarak ve devamlı olarak gündeme getirerek bir sonraki siber terör eylemlerinde toplumda infial oluşturmayı kolay hale getirmeyi amaçlamaktadır. Sosyal medya, güvenlik güçlerinin aciz olarak gösterilmesinin yanı sıra toplumda sürekli olarak korku ve panik havası yaratmakta ve terör örgütlerine hiç bir şey yapmadan amaçlarına ulaşma imkânı sunmaktadır.

Bu bağlamda terör örgütleri sosyal medyayı, kitlelere ulaşımının kolay olması, ucuz olması, gizlenmesinin kolay ancak tespit edilmesinin zor olması, toplumları yanlış yönlendirilmesi için trol hesaplarla kamuoyu oluşturulabilmesi, hedeflere uzaktan erişimin kolay olması gibi nedenlerle tercih etmektedirler.

#### **4. Terör Örgütleri – Asimetrik Siber Uzay Kullanımı İlişkisi**

Gerek gerçek kimlik bilgilerin verilme zorunluluğunun olmaması, gerekse de kimlik tespitinin çok zor olması ve küçük bir uğraşı ile çok geniş kitlelere ulaşabilme imkânı vermesi gibi avantajlar terör örgütlerinin siber uzaya yönelmelerine neden olmaktadır. Siber uzayın teröristlere düşük maliyet, az kişi, gizlenme ve uzaktan faaliyet imkanı gibi kolaylıklar sunmasının yanı sıra yüksek kazanç elde etmelerine imkan vermesi asimetrikliğe neden olmaktadır. Ayrıca siber uzayda



işlem yapmada terör örgütlerinin herhangi bir kurala veya kanuna bağlı kalmak zorunda olmamalarına karşın devlet ve vatandaşların uyması gereken birçok kanun, yönetmelik ve uluslararası antlaşmaların olması asimetrikliği arttırmaktadır.

Bu bağlamda terör örgütleri asimetrik siber uzayı uyması gereken kuralların olmaması, kimlik tespitinin zor olması, geniş kitlelere kolay ulaşma imkânı sunması gibi nedenlerle tercih etmekte ve silah olarak ta sosyal medya ve haber sitelerini kullanmaktadırlar. Eğer bu iki ortamda istedikleri etkiyi yaratamazlar ise servis dışı bırakma, kimlik avcılığı, ortalama saldırıları, bilinen açıklıkları kullanarak sistemlere sızma gibi yöntemlere yönelebilirler. Dolayısı ile istenilen hedefe ulaşmada siber uzay oldukça esnek yöntem geçişleri sağlamaktadır.

## **5. Geleneksel Terör ve Siber Terör Seçim Nedenleri**

Geleneksel terörde kurban olarak seçilen kişi veya kurum ile fiziksel bir irtibat söz konusudur; fakat siber terörde teknoloji ve internet sayesinde hedefe yaklaşılmadan ve hedef bölgesine intikale gerek kalmadan ve gerçek kimliği belli etmeden eylem gerçekleştirilebilmektedir. Ayrıca geleneksel terör eylemlerinde kullanılacak patlayıcı ve silah sistemlerini kullanılabilmesi için çok sayıda örgüt mensubuna, satın alabilmek için de yüksek meblağlara ihtiyaç duyulması ve bu paranın diğer suç teşkil yollardan ulaşılmaya çalışılması riskleri arttırırken, siber saldırının sadece bir kişi tarafından silah sistemleri ile karşılaştırıldığında hiçbir maliyeti olmayan bir bilgisayar ile gerçekleştirebilmesi siber terör eylemlerini daha cazip kılmaktadır. Fayda maliyet boyutunun yanı sıra geleneksel

terör eylemi belirli bir alanda gerçekleştirilirken siber terör sınırsız bir seçim alanı ve yüksek etki yaratacak kritik altyapı varlıklarını sunmaktadır.

Terör örgütleri, örgüt üyelerinin barınması, iaşesi, eğitimi, örgüte yeni üye kazanımı gibi işlemler için ve özellikle bu işlemleri gizli şekilde gerçekleştirebilmek için çok fazla para harcamaktadır. Buna karşın teknolojiadaki gelişmelerin ulus devletlere İnsansız Hava Aracı (İHA) gibi yenilikler sunması terör örgütlerinin kamplarını, lojistik uygulamalarını, kırsaldaki hareketlerinin takip edilmesine, yeni üye kazanma faaliyetlerinin sekteye uğramasına dolayısı ile eylemlerin sınırlı bir şekilde gerçekleştirilmesine neden olmaktadır. Buna karşın siber uzay terör örgütlerine psikolojik ve sosyolojik bilgilerle hazırlanmış görseller ile tespiti zor sempatican, üye ve militan temin etmesine, üyelerini bir araya getirmeden eğitmesine, üyelerini iletişimi koparmadan kırsal alan yerine kentsel alanlarda barındırmasına olanak sağlamıştır. Terör eylemlerinde ise havaalanı bombalama veya uçak kaçırma gibi zor bir eylem yerine dünyanın bir ucundan havayolu bilgi sistemini veya uçuş kulelerinin bilişim alt yapısını devre dışı bırakma veya ele geçirme yöntemlerini kullanmaya başlamıştır.

Bu bağlamda siber terörün klasik teröre karşı seçilmesinin nedenleri: Klasik terörde kurban ile fiziksel temasa geçilmesinin gerekliliği, siber terörde ise teknoloji ve internet sayesinde hedefe yaklaşmadan ve kimliğini belli etmeden faaliyetlerini gerçekleştirilebilmesidir. Klasik terörde silah satın almak için yüksek ücretlere ve alınan silahları kullanmak için çok sayıda örgüt elamanına ihtiyaç

duyulmaktadır. Siber terörde ise saldırıyı bir kişi bile gerçekleştirebilmektedir. Klasik terör belirli bir alanda gerçekleştirilmekte iken siber terör küresel olarak gerçekleştirilebilmektedir. Etki olarak düşünüldüğünde siber terör kritik altyapı olarak değerlendirilen varlıkların kötü amaçlı kullanılmasıyla klasik terörden çok daha etkili olabilmektedir.

## **6. Terör Örgütleri için Siber Terörizmin Çekici Unsurları**

Küreselleşme ile siber terörizmin çekici unsurları az maliyete çok etki yapabilmesi, dağınık ve bağımsız militanlarca yapılabilmesi, bir anda ortaya çıkma ve hemen akabinde kaçılabilmesi, eylemlerin önceden tahmin edilememesi, masum insanları kullanarak hedef saptırabilmesi, çok sayıda hedef sunması, kanun ve kurallara takılmadan ilerleme imkânı vermesi, geniş kitlelere çok kolay ulaşma imkânı vermesi ve daha birçok alanda kolaylıklar sağlamasıdır.

## **7. Siber Terörizmin Tehdit Potansiyeli**

Teknolojinin aktif kullanımı gündelik yaşamı kolaylaştırmanın beraberinde ulusal ve uluslararası ilişkilerde ve toplum yaşantısında bir takım negatif etkiler de ortaya çıkarmaktadır. Her an tetikte bekleyen terör örgütleri de eylemlerini gerçekleştirebilecekleri alanlar araştırmaktadır. Terörizmin doğasında var olan az maliyetle büyük etki oluşturma asimetrikliği, terör faaliyetlerini siber uzaya taşıyan en önemli etkenlerden biridir. Çünkü terörist gruplar az bir güçle devletlere karşı gelmeye çalışmaktadır. Siber uzayda asimetrikliğin boyutu tartışılrsa da asimetrikliğin oluşu muhakkaktır. Küçük saldırı gruplarının devlet gibi büyük bir organizasyona onu aciz gösterecek

nitelikte çok büyük zarar verebilme çabası terör örgütlerini siber uzayın potansiyellerini kullanma ihtiyacına yöneltmiştir. Bu potansiyel alanlar:

- \* Devletler için klasik savaş ve ordular ile istihbarat servisleri aşırı maliyetlidir ve resmi uluslararası ilişkiler devletlerin gizli hedefleri açısından istenildiği ölçüde verimli değildir.
- \* Her ne kadar siber savaş boyutuna girse de, devletler diğer devletlere resmi memurları aracılığı ile saldırı yapmaktansa terör örgütlerini veya örgüt iltisaklı kişilerce eylem yaptırmaktadır. Böylelikle artık fail devlet ya da gizli servis değildir terör örgütü veya terör örgütü üyesi olmaktadır.
- \* Terör örgütleri kirli paralar ile profesyonel anlamda toplum mühendisliği desteği alarak sosyal medya vasıtası ile toplumlara kolayca yönlendirilebilme imkânına kavuşmaktadır.
- \* Terör örgütleri belirli bir noktaya saldırı gerçekleştirmektense ulaşım, finans, iletişim, enerji, medya gibi sistemlerin bilişim alt yapılarını çökerterek çok daha fazla etki yaratmakta, toplumda kargaşa ve infiale neden olabilmektedir.
- \* Akıllı teknoloji ürünlerinin kullanımının artması, Nesnelerin İnterneti<sup>129</sup> (Internet of Things (IoT), network sistemleri ve akıllı mobil cihazlarla bilgi toplama artık çok daha kolaydır.

---

<sup>129</sup> 1999 yılında Kevin Ashton tarafından öne sürülen ve günlük hayatta kullanılan tüm araç gereçlerin kendi aralarında kablosuz ağlar üzerinden iletişim halinde olmasıdır. Bkz. Barış, Öztuna, **Endüstri 4.0 (Dördüncü Sanayi Devrimi) ile Çalışma Yaşamının Geleceği**, Gece Yayınları, 1.Baskı, Ankara 2017, s.69.

Bu bağlamda siber terörizmin tehdit potansiyeli geleneksel teröre nazaran çok daha fazladır. Siber terör ile internet bağlantıları, elektrik akışı kesilebilmekte, havaalanlarında uçakların iniş ve kalkışlarında sorun çıkartılabilmekte, barajların suyu boşaltılabilmekte, kurumsal veya özel bilgilere ulaşılabilenekte, su kesintisi oluşturulabilmekte, trafik ışıkları değiştirilerek bir şehrin trafiği kilitlenebilmekte ve bankalardaki hesaplar boşaltılabilmektedir. Dördüncü Sanayi Devriminin yeniliği olan nesnelere interneti ile artık siber teröristler önlem alınmazsa insanların yatak odalarına bile girebilir düzeye gelecektir.

## **8. Siber Terörizmin Türkiye Üzerine Etkileri**

Diğer tüm ülkelerde olduğu gibi Türkiye’de de hayat pahalılığından kaynaklı olarak siber güvenlik uygulamaları ikinci plana itilmektedir. İnsanlar siber güvenliğe harcanan parayı gereksiz olarak değerlendirmekte veya ihtiyaç listesinin sonuna atmaktadır. (Özellikle daha önce bir etkisini görmediyse) Buna ek olarak siber güvenlik konusunda bütün dünyada olduğu gibi Türkiye’de de yetişmiş personel sıkıntısı olduğu değerlendirilmektedir. Bu bağlamda siber terör eylemlerinin hedefi olabileceği değerlendirilen boyutlar:

- \* ‘‘e-Devlet uygulamaları,
- \* Ulaşım, finans, bilişim, iletişim, enerji alt yapı sistemleri, baraj gibi kritik yapılar,
- \* Terör örgütleri tarafından sosyal medyanın bireylerin hassas noktalarının tespit edilerek toplumun analiz edilmesi,

yönlendirilmesi, farklılıkların değerlendirilmesi ve devlet aleyhine kamuoyu oluşturma çalışmaları,

- \* Kültürel değişim ve yozlaştırma çabaları
- \* Yalan ve yönlendirici haber yayma çalışmaları
- \* Kurumlar ve personel hakkında çok önemli seviyedeki bilgilerin sızdırılması çalışmaları,
- \* Eğitimsiz ve bilinçsiz personel zafiyetinden faydalanarak kapalı sistemlere yerel sızıntı ve saldırı çalışmaları,
- \* Güvenlik unsurları başta olmak üzere kamu kurum ve kuruluşlarının WEB sayfalarının ele geçirme çabalarıdır.

## **9. Siber Güvenlik Konusunda Kurumlara ve Bireylere Düşen Görevler**

- \* Kurumlar çalışanlarını siber güvenlik önlemlerinin ulusal güvenliğin de bir parçası olduğu konusunda bilinçlendirmelidir.
- \* Bireyler çalıştıkları kamu veya özel işletme ağlarının güvenliğinde bütüncül bir yaklaşım sergilemeleri konusunda teşvik edilmeli, bu ağlarda yaşanacak veri sızıntısının siber teröristlerce ulusal güvenliğe karşı kullanılacağı konusunda bilinçlendirmelidir.
- \* Kurumlarının kullandığı bilişim altyapı ağlarının kontrol ve denetimlerinin Sürekli Güvenlik İzleme Çatısı<sup>130</sup> (Continuous

---

<sup>130</sup> Sürekli Güvenlik İzleme Çatısı kavramı kurum ve kuruluşlardaki bilişim sistemlerinin sürekli olarak gözlenmesi için oluşturulmuş bir yöntemdir. Seçilmiş ölçümlerin toplanıp, raporlandıktan sonra analiz edilerek kurumların güvenlik

Security Monitoring - CSM) süreci ile sürekli yapılması için hangi birimin sorumlu olduğu belirlenmeli veya bu konuda hizmet veren özel şirketlerden hizmet alınmalıdır. Bu bağlamda en temel amaç siber güvenlik mekanizmaları arasında kör nokta bırakmamaktır.

- \* Kurumlar her şeyden önce öz yetenekleri (core competence) kapsamında en kritik varlıklarını ve bu varlıklara ulaşma yollarını belirlemeli, bir saldırgan veya teröristin kurum ağına sızdığı anda ise elde etmek isteyeceği veri veya sistemleri nesnel bir risk analizi ile değerlendirerek muhtemel sistem açıklarını ortaya koymalıdır. Çünkü siber uzayda etkin siber savunma önlemleri almak, terörist gibi düşünebilmeyi gerektirmektedir.
- \* Çalışanlar internet üzerinde kendisi ve kurumuna ait bilgileri ifşa etmemeleri konusunda bilinçlendirilmelidir.
- \* Genel internet ağına direkt bağlı kurumlarda çalışanlar özellikle oltalama saldırılarına karşı teknik düzeyde bilgilendirilmelidir.
- \* Çalışanlar, siber terörizme karşı alınan önlemlere sürekli olarak uymalı ve stratejileri benimsemelidir.
- \* Başta Türk Silahlı Kuvvetleri (TSK) olmak üzere tüm güvenlik birimleri açısından siber uzay 5'inci muharebe alanı olarak kabul edilmeli ortaya çıkan tehdit ve fırsatlara yönelik

farkındalık eğitimleri düzenlenmeli, siber operasyonlar konusunda akademik çalışmalar takip ve teşvik edilmelidir.



## SONUÇ VE ÖNERİLER

### 1. Sonuçlar

*“Değişen dünya dengeleri ve uluslararası ilişkilerdeki farklılaşmalar sonucunda, sıcak savaşlar, yerini soğuk savaş metotlarına ve vekâlet savaşlarına bırakmıştır. Soğuk Savaş döneminde iyice belirginleşen ve sofistike yöntemlerle geliştirilen psikolojik savaş türü ve bu savaşın vazgeçilmez unsuru olan düşük yoğunluktaki çatışmalar, terör ile ilgili akademik çalışmaların artışı da beraberinde getirmiştir.”<sup>131</sup>*

Literatür taraması sonucunda elde edilen bilgiler ışığında dünyanın yeniden şekillendiği değerlendirilmektedir. Birbirinden bağımsızmış gibi görünen bu üç kavramın aynı süreç içerisinde bir araya gelmesi bilişim teknolojilerinin de gelişmesi ile ulusal ve uluslararası ekonomik, politik, demografik, sosyo-kültürel dengeleri tümüyle değiştirmektedir. Söz konusu süreçler arasındaki etkileşim ve bunların yol açtığı tepkiler bilgi ve ağ toplumunun oluşmasına, ekonominin küresel düzeyde değerlendirilmesine ve sanal dünya ortamının yaratılmasına neden olmuştur. Bunun sonucunda ulusal ve uluslararası sermayenin yeniden paylaşılması, teknolojinin çok hızlı gelişmesi, küreselleşmenin negatif yönde etkileri ve ayrıca milliyetçiliğin teşvik edilmesi yeni bir küresel terörizm çeşidi olan siber terörizm kavramını ortaya çıkarmıştır.

---

<sup>131</sup> Osman Vedüd Eşidir ve Gökhan Bak, “Şiddet Unsuru Olarak Terör Olaylarının Medyada Haberleştirilmesi”, *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, Cilt: 5, Sayı: 7, 2018, s. 14.

İkinci Dünya Savaşı sürecinde değeri daha fazla anlaşılan ve savaştan sonra gelişimi hız kazanan bilişim teknolojilerinin ve doğal olarak iletişim araçlarının katkılarıyla bilgi, haber ve mesajlar anlık olarak iletmeye başlanmış ve bunun sonucunda bilgi ve ağ toplumu aşamasına gelmiştir. Bu gelişmeler sonucunda toplumların sosyo-kültürel yapılarında yavaş fakat kökten değişiklikler ortaya çıktığı değerlendirilmektedir. Bu değişiklikler toplum tarafından benimsedikçe hız kazanmıştır. Bu bağlamda bilgi ve ağ toplumlarının hızlı toplumsal dönüşümlere yeterince çabuk adapte olamamaya başlamaları sonucunda toplumu oluşturan bireylerde gelecek korkusu, bireysel ve örgütlü terörün kolay ve yaygın hale gelmesi, özel hayata müdahale edilmesi ve bireylerin mahremiyetine toplum düzenini sağlamak adı altında devletlerin de etki edebilecek şekilde teknolojik alt yapıyı oluşturmasının geleceğe dair endişeleri arttırdığı değerlendirilmektedir.

Bu yeni dünya düzeninde toplumsal yapı, küreselleşmenin etkisi ile birlikte kültürel değişimlere neden olmakta, bazı kesimlerde zenginlik yaratmakta, bazı kesimlerde ise eşitsizliklere ve açlığa neden olmaktadır. Bununla beraber küreselleşme süreci, ulus-devleti yapısını ve etkisini küçültüp, sınırları gereksiz göstermekte ve kaynağı farklı da olsa karşılıklı bağımlılık ilişkileri yaratmaktadır. Bu bağımlılıkta ise güçsüz ortak sömürülmeye, güçlü ortak ise tüm kaynaklara sahip olmanın yanı sıra güçsüz ortağın iç işlerine bile karışmaya başlamaktadır.

Terörizm, hedefler, hedeflerine ulaşmada kullandığı yöntemler, kullandığı silahlar, örgüte sempatican ve finans kaynağı bulma ve örgütlenme biçimleri yönünden bir farklılaşma yaşamaktadır. Son zamanlarda haberlere de yansıyan teknoloji destekli terör saldırılarının meydana geldiği birçok ülkede onlarca masum insanın öldüğü ve saldırıların teknoloji ile sıkı ilişkisi olduğu için insanlık namına küresel ölçekte yeni bir tehdit unsuru oluştuğu görülmektedir. Oluşan bu tehdit unsurunun ilk olarak teknoloji yönünden daha az gelişmiş ülkelerin zengin ve güçlü ülkelere karşı milliyetçi tavır takınmasına, ikinci olarak ta terör örgütlerinin yakalanmasının daha zor olması nedeniyle teknolojiye yönelmesi şeklinde değerlendirilmektedir. Bu bağlamda insanlık yararına üretilen teknolojinin kötü düşüncelere sahip beyinler tarafından şahsi ve örgütsel çıkarlar uğruna kullanıldığı ve adeta bilgi üreten ülkelerin kendi üretmiş oldukları bilgi ile vuruldukları değerlendirilmektedir.

Bireylerin yanı sıra devletlerin güvenliği de son derece kırılgandır. Bu kırılganlık olgusu dünyada pek çok ulusun kendini güvensiz bir ortamda olduğu hissine yol açmaktadır. Tarihsel süreçte olduğu gibi günümüzde de Batı coğrafyasının dışında kalan halklar, herhangi bir Batılı ülkenin doğrudan çıkarını temsil etmedikleri sürece sürekli risk altında olduğu hissiyatı ile yaşamlarını sürdürmektedirler. Sürekli risk altında olma düşüncesi dünya üzerindeki güvenlik algısına ve bunun gölgesinde kurulan güvenlik pratiklerine dönük bir tepkinin doğmasına yol açmaktadır.

Yeni tip terör olarak dile getirilen siber terör kavramı, klasik terörden farklı olarak yukarıda bahsedilen güvensizlik algısını hep canlı tutmayı ve güvenlik algısını istikrarsızlaştırmayı hedef almaktadır. Klasik terör, bölge üzerinde hâkimiyet kurmak isteyen sömürgeci devletlerin desteği altında diğer devletlerin çıkarlarını tehdit ederken, siber terör dünya üzerindeki güvenlik algısını kırılganlaştırmaya çalışmaktadır. Çünkü artık devletlerin karşısında kendisini açıkça tehdit eden örgütler değil, itibarını, gücünü, yönetim şeklini ve felsefesini tehdit eden örgütler bulunmaktadır. Bu bağlamda hedeflerine gizlilik içinde ve ışık hızında ulaşma imkânına kavuşabilen terör örgütlerinin ileriki zamanlarda oldukça yıkıcı bir siber terör eylemini gerçekleştirebilecek potansiyele sahip olabileceği değerlendirilmektedir. Çünkü terörün radikal dini inançtan beslenen ideoloji yönü, maddi gücü ve organize olabilme kabiliyetini, gelişen bilişim teknolojileri ile birleştirdiğinde nereden ve nasıl geldiği belli olmayan birçok siber terör saldırılarına imkân sağlayacaktır.

Uluslararası terör, bilişim teknolojileri sayesinde siber uzayda tespit edilemeyen ve caydırılmayan bir nitelik kazanmıştır. Tablo 2’de gösterildiği üzere, internet siteleri üzerinden hedeflerine ulaşmaya çalışan örgütler destek unsurları ile beraber bir sanal devlet yapılanması altında değişik coğrafyalarda ortak bir ideoloji ile hareket etmekte, örgütün alt birimleri bölgesel seviyede kendini yeniden düzenleyerek faaliyetlerini sürdürmektedirler. Bu örgütlerde hiyerarşik örgüt yapılanması çok katı olmadığı gibi, örgütün uç birimleri, söz konusu ideoloji ile bazen inisiyatif alarak, kontrol biriminin bilgisi dışında terörist eylemlere girişebilmektedirler.

Sonuç olarak, bilişim teknolojisi devriminin toplumsal yapıyı dönüştürmesi, zaman ve mekân kavramlarını sanal ortamda tekrar inşa etmiş ve ağ toplumunu ortaya çıkarmıştır. Bu bağlamda kapitalizm ve devletçilik olguları yeniden kavramsallaşmakla birlikte tekrarlayan krizler ve yaygın istikrarsızlıklar yüzünden küresel ekonominin çapı genişlemektedir. Bu genişlemenin, toplumsal eşitsizliklere, gelir dağılımı adaletsizliklerine, dışlanmışlıklara ve anlamını yitiren ulus devlet yapılarına neden olduğu değerlendirilmektedir. Ağ toplumundaki bu negatif olgular diğer ideolojilere karşı örgütsel meydan okumalara ve ulusal/kültürel/dini özerk kimlikler inşa etmelere neden olmuştur. Böylece terör ve terörizmin boyutları değişmiş, küreselleşen dünyanın en ücra köşesine neredeyse masrafsız bir şekilde etki edebilecek düzeye gelmiştir.

Küreselleşme sürecinin bilişim, iletişim ve medya teknolojilerindeki yeniliklerin de etkisiyle hız kazanması terörizmin geniş kitleleri çok daha kolay, hızlı ve masrafsız bir şekilde etkilemesine, yeni hedef ve düşmanlar yaratmasına, bireysel ve toplumsal travmalara neden olmaktadır. Bu kitapta iki ayrı dinamik süreç olan terörizm ve küreselleşme kavramlarının birbirini besleyen kavramlar olduğu sonucuna ulaşılmıştır. Çünkü küresel terör örgütleri siber uzayı kullanarak destekçileriyle birlikte bir sanal devlet yapılanması oluşturmakta ve örgütün alt birimleri bölgesel bağlamlarda kendilerini yeniden düzenleyerek faaliyetlerini gerçekleştirebilmektedirler. Örgütün yumuşak bir şekilde oluşturduğu hiyerarşik yapılanma sayesinde tüm alt birimler birbirleriyle haberleşmeyi sanal ortama taşımakta ve böylece fiziksel olarak bir araya gelmeyen, yakalanması

ve tespit edilmesi zor bir yapılanma ortaya çıkmasına neden olmaktadır. Ayrıca, siber uzay ortamında terörizmin küreselleşmesi, bölgesel terör örgütlerinin gelişen teknolojiye maksimum seviyede yararlanmasının yolunu da açmakta olup, tek bir teröristin bile küresel ölçekte eylem ve saldırı yapabilmesine olanak sağlamaktadır.

## **2. Öneriler**

Her şeyden önce, batı devletlerinin ve uluslararası sermayeye hükmedenlerin kârını gözeterek ekonomik küreselleşme yerine küreselleşmenin istihdam, işsizlik, yoksulluk ve açlığı ortadan kaldıracak şekilde insani ve sosyal boyutu öne çıkarılmalıdır.

Yeni bir terör türü olarak ifade edilen siber terörden sakınmak için sadece kurumlar veya devletler düzeyinde mücadele etmek değil, aynı zamanda terörün devletlerin eksikliklerinden ve yeni dünya düzeninin sıkıntılı yönlerinden istifade etmekte olan ideolojik akımları ile de mücadele etmek gerekmektedir.

Bu mücadelede sadece konuyu bilen uzmanlar değil, son kullanıcı rolündeki bireyler de bu güvenlik tedbirlerinden haberdar kılınmalıdır. Bu bağlamda televizyonlarda yayınlanan zorunlu reklamlar içerisinde halkın dikkatini çekmek amacıyla siber uzayda oluşan tüm tehditler belirtilmeli, siber teröre karşı alınacak önlemler konusunda toplumsal bilinç seviyesinin artırılması sağlanmalıdır.

Geleceğin teröristleri ve ele başları günümüzdeki örneklerinden farklı olarak sayısal ve sanal bir dünya içerisinde doğacak ve bilişim teknolojilerini daha kolay kullanacak şekilde yetiştikleri için siber

saldırıları daha profesyonel şekilde gerçekleştireceklerdir. Yetkin olacakları siber uzay ve bilgisayar bilgisi sayesinde, siber terör eylemlerindeki potansiyeli keşfedebileceklerdir. Teknolojinin son yıllarda özellikle bilişim teknolojilerinde müthiş bir ilerleme gösterdiği ve geliştirilmesi planlanan yazılımlar ve donanımlar dikkate alındığında siber terörizmin daha çekici ve etkili bir hal alabileceği değerlendirilmektedir. Bu bağlamda gelecekte bilişim sistemleri yeterince güvenli hale getirilmediği takdirde, siber uzayda gerçekleştirilen eylemlerin gerçek dünyada çok daha fazla etkiler yaratacağı değerlendirilmektedir.

Siber terörün neden olacağı kayıpların siber güvenlik önlemleri kapsamında yapılacak harcamalardan çok daha fazla olabileceği dikkate alındığında, öncelikle devlet, kurum ve kuruluşların sonrasında ise bireylerin siber güvenlik önlemlerine daha fazla bütçe ayırması gerektiği değerlendirilmektedir. Bu bağlamda bilgisayarlarda orijinal yazılım kullanılmasının zorunlu olduğu gibi koruyucu anti virüs yazılımları kullanımı da zorunlu hale getirilmesinin uygun olacağı değerlendirilmektedir.

Son kullanıcıların bilgisayarlarının yanı sıra cep telefonlarında da bir anti virüs yazılımı bulundurmasının onları virüslere ve bilgisayar korsanlarına karşı koruyacağı değerlendirilmektedir.

Siber saldırılardan korunmanın en temel ilkesi kullanılan yazılımda açık kapıların olmamasıdır; ancak bu neredeyse imkânsızdır. Bu nedenle, Windows ve IOS gibi işletim sistemlerine bağımlı kalmaktansa Linux ve Pardus gibi özgür ve açık kaynak kodlu işletim

sistemlerine yönelmenin, popüler işletim sistemlerindeki açık kapılara maruz kalmayı ortadan kaldıracığı değerlendirilmektedir. Bunun yanı sıra Whatsapp gibi popüler sohbet yazılımları yerine Chat-In ve Türkcell BİP gibi güvenilir yerli sohbet yazılımlarının kullanılması kişisel bilgilerin ve sohbetlerin ifşa edilmemesi açısından önemlidir. Hotmail, Gmail ve Yahoo gibi hemen hemen herkesin kullandığı e-posta hesaplarından kaçınılması gerektiği de değerlendirilmektedir. Çünkü siber terör örgütlerinin yanı sıra küresel şirketler müşteri ilişkileri yönetimi açısından bireylerin alışveriş alışkanlıklarını ve ziyaret ettikleri siteler hakkında bilgi toplamaktadırlar.

Siber saldırılardan korunmada bireysel önlem olarak kullanılan şifrelerin kolay tahmin edilemeyen, büyük harf, küçük harf, rakam ve noktalama işareti içerecek şekilde karmaşık seçilmesi gerekmektedir. Oluşturulan bu parolalar asla sosyal ağ platformları ve e-posta hesaplarında kullanılmamalı ve Google tarafından “Parolayı Hatırla” seçeneği seçilmemelidir.

Akıllı telefonlara ve tabletlere indirilecek yazılımlara dikkat edilmeli ve sahte uygulama indirmekten kaçınılmalıdır. Telefonlardaki uygulama izinlerini kontrol etmek çok önemlidir. Birçok akıllı telefon uygulamasının içerisinde kişisel verileri toplayan ve veritabanlarına gönderen arka kapıların mevcut olduğu bilinen bir gerçektir.

Tehdit tanımları artık Soğuk Savaş dönemindeki gibi sadece askeri yönden değil, teknolojik gelişmişlik, bilgiye sahip olma, ekonomik güç ve enerji kaynaklarını da içine alan bir tanımla yapılmaktadır. Buna ek olarak tehdit unsurunun kaynağı ve ortaya çıkacağı yerin belli



olmaması etkin önlemler alınmasını da güçleştirmektedir. Buna bağlı olarak siber saldırılar, ağ ve bilgi güvenliği, milli güvenlik ve devlet politikalarında yeni alanlar açarak sorunun daha da karmaşık bir hale gelmesine neden olmaktadır. Bu sebeple milli güvenliğin sağlanabilmesi için diğer milli güç unsurlarının yanı sıra, teknolojik gücün geliştirilmesine daha fazla katkıda bulunulması gerektiği değerlendirilmektedir.

Siber terör eylemlerinden zarar görmemek için kurum ve kuruluşlar personelini yeterli seviyede eğitmeli, personel kurum içi ağa yabancı veya şahsına ait USB takmaması konusunda devamlı olarak uyarılmalıdır.

Personele, kötü niyetli kişi veya örgütlerce kullandıkları akıllı cep telefonlarının heklenerek ortam dinlemesi veya görüntü alınması yoluyla istihbarat sızıntısına neden olunmaması yönünde eğitimler verilmeli, telefonların kurumların ilk girişlerinde bırakılması yönünde önlemler alınmalıdır.

Siber teröristlerin, elektromanyetik ışıma yoluyla veri elde etme yeteneklerini engellemek için, bina içindeki ve dışındaki tüm kablolar korunaklı tip seçilmelidir. Yabancı devlet destekli casus solucan robotların kanalizasyonlardan ilerleyerek havalandırma boşluğuna yakın kablolardan bilgi çalabileceği hatırlanmalı, gerekirse intranet ağı bina havalandırma boşluğundan uzak olacak şekilde döşenmelidir.

Kurum ve kuruluşlara girişlerde kullanılmak üzere, insan vücuduna enjekte edilmiş çok küçük sinyalleri bile tespit edebilen detektörler üretilmelidir. Hatta giriş noktalarında Covid-19 salgınında kullanılan

termal kameraların daha da geliştirilerek kişilerin olağan dışı heyecan, korku, stres gibi dışa vurum jest ve mimiklerini tespit edebilecek kameralar üretilip kullanılmalıdır.

Sonuç olarak, ulusal büyük veri ve bilgi altyapısı oluşturulurken geleceğe yönelik bir vizyon içerisinde, hem teknik, güvenlik tedbirlerinin tesisinde hem de yasal düzenlemelerde siber terör gerçeğinin daha gerçekçi bir şekilde ele alınmasının gerekliliğinin büyük önem taşıdığı değerlendirilmeli ve tüm devlet, kurum ve kuruluşlarca dünyadaki en zayıf güvenlik unsurunun insan olduğu asla unutulmamalıdır.

Havelsan ve Aselsan gibi yerli ve milli kurumlar siber terörizme ve siber savaşa karşı bilişim alt yapılarını korumak maksadıyla yerli ve milli yazılımlar üretmelidir. Bu yazılımların devlet desteği ile tüm kamu kurum ve kuruluşlarda kullanımının yaygınlaşması sağlanmalıdır.

Yerli ve milli yazılımların testi için öncelikle ödüllü bir yarışma düzenlenmeli, yazılımları hekeleyebilenlere ödüller verilmelidir. Hatta yazılımı hekeleyebilenler, devlet siber ordusuna katılmaya davet edilmelidir.

## KAYNAKÇA

### Kitaplar

Altan, Mehmet, **Küresel Vicdan**, Timaş Yayınları, 1.Baskı, İstanbul 2011, 159s.

Altunok,Taner ve Sökmen, Aşkın İnci, **Dünya'dan Siber Terör Örnekleri: Suç, Terör ve Savaş Üçgeninde Siber Dünya**, Ed: Haydar Çakmak ve Taner Altunok, Barış Platin Kitabevi, Birinci baskı, Ankara 2009, 232s.

Bayraktar, Gökhan, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, Yeniüzyıl Yayınları, 1. Baskı, İstanbul 2015, 232s.

Burnst, Phillip W., **Use of the Internet by Terrorists-A Threat Analysis: Responses to Cyber Terrorism**, Edited by Centre of Excellence Defence Against Terrorism, Ankara Turkey, IOS Press, Amsterdam 4-5 October 2007, s.34-60.

Canberk, Görol ve Sağırođlu, Şeref, **Bilgi ve Bilgi Güvenliđi Casusu Yazılımlar ve Korunma Yöntemleri**, Grafiker Ltd.Şti, 1. Baskı, Ankara 2006, 480s.

Clifford,R.D., Cybercrime, Carolina Academic Press, Durham, 312s.

Çakır,Hüseyin ve Kılıç,Mehmet Serkan, **Güncel Tehdit: Siber Suçlar**, Seçkin Yayınevi, 1. Baskı, Ankara 2014, 327s.

Çakmak,Haydar ve Demir,Cenker Korhan, **Siber Dünyadaki Tehdit ve Kavramlar: Suç, Terör ve Savaş Üçgeninde Siber Dünya**,

Ed: Haydar Çakmak ve Taner Altunok, Barış Platin Kitabevi, 1. Baskı, Ankara 2009, 232s.

Çiftci, Hasan, **Her Yönüyle Siber Savaş**, Tübitak Popüler Bilim Kitapları, 1. Baskı, Ankara 2013, 394s.

Denning, Dorothy E., “Activism, Hacktivism and Cyberterrorism: The Internet as a Tool For Influencing Foreign Policy Decision Making”, **Network and Netwars: The Future of Terror, Crime and Militancy**, Sekizinci Bölüm, Ed.: John Arquilla ve David Ronfeldt, Rand Corporations, San Francisco 1999, s.239-288.

Denning, Dorothy, **Information Warfare and Security**, Addison Wesley, 1. Baskı, New York, 1999, 544s.

Drori, Gili S., v.d., **Globalization and Organization**, Oxford University Press, 1. Baskı, New York 2006, 339s.

Eren, Erol, **Stratejik Yönetim ve İşletme Politikası**, Beta Yayıncılık, 8. Baskı, İstanbul 2010, 578s.

Güneştaş, Murat, v.d., **Siber Terörizm: Motivasyon ve Yöntem, Siber Suçlar: Tehditler, Farkındalık ve Mücadele**, Ed: Fatih Tombul, Murat Güneştaş ve Oğuzhan Başbüyük, Global Politika ve Strateji Yayınları, 1. Baskı, Ankara 2015, 335s.

Kaldor, Mary, **News and Old Wars**, Standford University Press, 2. Baskı, California 2007, 224s.

Keleştemur, Atalay, **Siber İstihbarat**, Level Yayınevi, 1. Basım, Kocaeli 2015, 472s.

Mattelart, Armand, **Mapping World Communication: War, Progress, Culture**”, Minneapolis, University of Minnesota, Minnesota 1994, 294s.

Marks, Karl ve Engels, Friedrich, **Kominist Manifesto**, Çev.: Celal Üster ve Nur Deriş, Can Yayınları, E-Kitap 1. Baskı, İstanbul 2014, 149s.

Öztuna, Barış, **Endüstri 4.0 (Dördüncü Sanayi Devrimi) ile Çalışma Yaşamının Geleceği**, Gece Yayınları, 1.Baskı, Ankara 2017, 155s.

Record, Jeffry, **Bounding The Global War on Terrorism**, Strategic Studies Institue, US Army War College, Aralık 2003, 64s.

Sieber, Ulrich, **The Threat of Cybercrime**, In Council of Europe Ed: Organised Crime in Europe, Strasbourg: Council of Europe Publishing, Situation Report 2004, Bölüm 3, s.81-218.

Singer, P.W. ve Friedman Allan, **Siber Güvenlik ve Siber Savaş**, Çev:Ali Atav, Buzdağı Yayınevi, 1. Baskı, Ankara 2015, 396s.

Şahin, Güngör, **Küresel Güvenlik ve NATO Teori-Aktör-Tehdit-Risk**, Detay Yayıncılık, 1. Baskı, Ankara 2016, 320s.

Thorton, Thomas Perry, **Terror as a Weapon of Political Agiation: Internal War**, Ed:Harry Eckstein, The Free Press, New York 1964, s.71-99.

Yalçınkaya,Haldun, **Savaş:Uluslararası İlişkilerde Güç Kullanımı**, İmge Kitabevi,Ankara 2008, 383s.

Wilkinson,Paul, **Terrorism versus Democracy**, Routledge, London  
2006, 254s.

Wilson, Clay, Computer Attack and “Botnets, Cybercrime and  
Cyberterrorism: Vulnerabilities and Policy Issues for Congress”,  
**Congressional Research Service The Library of Congress**, 29  
Ocak 2008, 45s.

### **Makaleler**

Abboth, Kenneth W. ve Snidal, Duncan, “Why States Act Through  
Formal International Organizations?”, **Journal of Conflict  
Resolution**, Cilt: 42, Sayı:1, Şubat 1998, s.3-32.

Aktel,Mehmet ve Gürkaynak, Muharrem, “Küreselleşen Terörizm: Bir  
Etkileşim Çalışması”, **38. ICANAS (Uluslararası Asya ve Kuzey  
Afrika Çalışmaları Kongresi)**, Sayı: 1, Cilt: 1, 2011,  
Ankara,s.77-88.

Avşar, Zakir, İnternet Çağında Medya, Terör ve Güvenlik, **TRT  
Akademi**, 2017/02/03, 19.12.2016, s.116-132.

Balaban, Özlem ve Okutan, Elvan Yıldırım, “Ekonomik Krizlerin Bir  
Sonucu Olarak Stratejik İşbirlikleri ve Şirket Birleşmelerinde  
Yönetmel Uyum Değerlendirilmesine Yönelik Bir Araştırma”,  
**Journal of Azerbaijani Studies**,  
Cilt: 12, Sayı: 1, 2009, s.299-310.

Başeren, Sertaç, H., “Terrorism with Its Differentiating Aspects”,  
**Defence Against Terrorism Review**, Cilt: 12, Sayı: 1, Bahar  
2008, s.1-12.

Baykal, Hülya ve Baykal, Tan, “Küreselleşen Dünya’da Çevre Sorunları”, **Mustafa Kemal Üniversitesi Sosyal Bilimler Dergisi**, 2008/5/9, 2008, s.1-17.

Bayzan, Şahin ve Özbilen, Alper, “Dünyada İnternetin Güvenli Kullanımına Yönelik Uygulama Örnekleri ve Türkiye’de Bilinçlendirme Faaliyetlerinin İncelenmesi ve Türkiye İçin Öneriler”, **5. International Computer & Instructional Technologies Symposium (20-22 Eylül 2011, Elazığ) Bildiriler Kitabı**, Fırat Üniversitesi, Elazığ 2011, s.253-260.

Brenner, Susan W. ve Goodman Marc D., In Defence of Cyberterrorism:An Argument for Anticipating Cyber-Attacks, **Journal of Law, Technology and Policy**, Cilt:1, 2002, s.1-57.

Bıçakçı, Salih, “Yeni Savaş ve Siber Güvenlik Arasında NATO’nun Yeniden Doğuşu”, **Uluslararası İlişkiler**, Cilt 9, Sayı 34, Yaz 2012, s.205-226.

Conway, Maura, “Reality bytes:Cyberterrorism and Terrorist “use” of the Internet”, **Department of Political Science**, Cilt: 7, Sayı: 11, 2002, s.1-17.

Delican, Mustafa, “Uluslararasılaşma ve Küreselleşme Bağlamında Karşılaştırmalı Endüstri İlişkileri: Gelişmeler ve Teorik Yaklaşımlar”, **Sosyal Siyaset Konferansları**, 2017/1/72, 20.02.2018, s.1-33.

Denning, Dorothy E., “Cyberterrorism”, **Global Dialogue**, 24 Ağustos 2000, s.1-10.

Denning, Dorothy E. ve Baugh William E. Jr., “Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism”, **National Strategy Informatin Center’s Working Group on Organized Crime (WGOC)**, 1997, s.1-33.

Eker, Sami “Savaş Olgusunun Dönüşümü: Yeni Savaşlar ve Suriye Krizi Örneği” **Türkiye Ortadoğu Çalışmaları Dergisi**, Cilt: 2, Sayı: 1, 2015, s.31-66.

Eşidir, Osman Vedüd ve Bak, Gökhan, “Şiddet Unsuru Olarak Terör Olaylarının Medyada Haberleştirilmesi”, **Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi**, Cilt: 5, Sayı: 7, 2018, s.13-32.

Fidanboy, Cemalettin Öcal ve Alan, Hale, “Kaynak Bağımlılığı ve Stratejik İşbirliği İlişkisi:Kaynak Özelliklerinin İş Birliği Oluşumuna Etkileri”, **Savunma Bilimleri Dergisi**, Cilt: 12, Sayı:1, Mayıs 2013, s.123-145.

Giacomello, Giampiero, “Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism”, **Studies in Conflict & Terrorism**, Cilt: 27, Sayı:5, 2004, s.387-408.

Golder, Ben ve George, Williams, “What is Terrorism? Problems of Legal Definition”, **University of New South Wales Law Journal**, Cilt: 27, Sayı: 2, 2004, s.270-295.

Kartal, Atahan Birol, “Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye’de DEAŞ ve ve YPG Örneği”, **Güvenlik Stratejileri Dergisi**, 2014/27, 16.04.2018, s.39-77.



Kartal, Çetin, “Küreselleşme Sürecinin Devlet Yapısı Üzerine Etkileri”, **Ankara Barosu Dergisi**, 2016/2, 22.06.2016, s.287-328.

Murray, Edwin A. Jr ve Mahon, John F. “Strategic Alliances: Gateway to the New Europe?”, **Long Range Planning**, Cilt: 26, Sayı: 4, 1993, s.102-111.

Nacos, Brigitte, “Terrorism/Counterterrorism and Media in the Age of Global Communication”, **United Nations University Global Seminar Second Shimame-Yamaguchi Session Terrorism – A Global Challenge**, 5-8 August 2006, s.1-19.

Pollitt, Mark M., “Cyberterrorism: Fact or Fancy?” **Proceedings of the 20th National Information Systems Security Conference**, October 1997, s. 285–289.

Shin, Seungwon, ve Gu, Guofei, Conficker and Beyond: A Large-Scale Empirical Study, **Proceedings-Annual Computer Security Applications Conference**, ACSAC, December 2010, s.151-160.

Tofangsaz, Hamed, “A New Approach to the Criminalization of Terrorist Financing and Its’ Compatibility with Sharia Law”, **Journal of Money Laundering Control**, Cilt: 15, Sayı:4, Ekim 2012, s.396-406.

Weimann, Gabriel, “www.terror.net: How Modern Terrorism Uses the Internet”, **United States Institute of Peace**, Special Report 116, Mart 2004, s.1-12.

Yorulmaz, Murat, ““Değişen” Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde “Değişmeyen” Güvenlik Paradoksu”, **Balkan Araştırma Enstitüsü Dergisi**, 2014/3/1, 2014,s.1-33.

### **İnternet Kaynakları**

Can Dündar, “Savaş şimdi de İnternette”, **Milliyet**, 22.07.2006  
[www.milliyet.com.tr/2006/07/22/yazar/dundar.html](http://www.milliyet.com.tr/2006/07/22/yazar/dundar.html)

Erişim Tarihi 11.10.2020

CNET, “Bad Flash Drive caused Worst U.S. Military Breach”,  
[http://news.cnet.com/8301-27080\\_3-20014732-245.html](http://news.cnet.com/8301-27080_3-20014732-245.html)

Erişim Tarihi: 08.11.2020.

Fingas, Jon,“One of the First True Computers is Finally on Public Display”, 25.11.2014, .[www.engadget.com/amp/2014-11-25-eniac-on-public-display.html](http://www.engadget.com/amp/2014-11-25-eniac-on-public-display.html) Erişim Tarihi: 08.11.2020

Hürriyet Haber: “Sezer:Türkiye'nin Lübnan'a asker göndermesine karşıyım”,25.08.2006,

[www.hurriyet.com.tr/gundem/4980763.asp?m=1](http://www.hurriyet.com.tr/gundem/4980763.asp?m=1).

Erişim Tarihi: 07.11.2020

<http://www.rutherfordjournal.org/article030109.html>

<http://egm.gov.tr/temuh/terorizm1.html> Erişim Tarihi 29.09.2020

[https://www.nato.int/cps/en/natohq/topics\\_52044.htm](https://www.nato.int/cps/en/natohq/topics_52044.htm)

Erişim Tarihi 26.12.2020.

<https://sozluk.gov.tr> Erişim Tarihi 29.09.2020.

<https://www.nato.int/nato-welcome/index.html>,

Erişim Tarihi: 30.10.2020.

<https://www.sabah.com.tr/teknokulis/haberler/2020/02/24/dunyada-ne-kadar-insan-internet-kullanıyor> Erişim Tarihi 29.09.2020

Nigel Stenley, Safety and Security in Industry 4.0 – Are You Ready,  
<https://www.infosecurity-magazine.com/opinions/safety-industry-4-1-1/> Erişim 15.10.2020

Scott Berinato, Cybersecurity-The Truth About Cyberterrorism, CIO  
From IDG, 15 Mart 2020. [www.cio.com/article/2440933/cybersecurity---the-truth-about-cyberterrorism.html](http://www.cio.com/article/2440933/cybersecurity---the-truth-about-cyberterrorism.html) Erişim  
Tarihi: 26.10.2020.

Serhat Kut, Sibermekanın Gerçekliği

<https://www.academia.edu/389859> Erişim Tarihi: 23.12.2020.

Taylor, Ian, “Russia accused of Unleashing Cyberwar to Disaple  
Estonia”, **The Guardian**, 12 Mayıs 2007.  
[www.theguardian.com](http://www.theguardian.com) Erişim Tarihi:08.11.2020

Warner, Bill, “Bill Warner Investigations Sarasota:Al-Qaeda Agents  
Anwar al-Awlaki, Ziyad Khaleel & Muneer Arafat Part of 9/11  
Hijackers Support Network in U.S.”, 21 Ocak 2019.  
[www.billwarnerpi.com](http://www.billwarnerpi.com) Erişim Tarihi: 07.11.2020

[www.amp.dw.com](http://www.amp.dw.com) Erişim Tarihi: 07.11.2020

[www.beyaz.net](http://www.beyaz.net) 25 Mart 2020 Erişim Tarihi:08.11.2020

[www.coğrafya.gen.tr/siyasi/jeopolitik](http://www.coğrafya.gen.tr/siyasi/jeopolitik) Erişim 24.10.2020

www.haberler.com Erişim Tarihi 07.11.2020

www.theage.com.au/articles/2003/04/07/104567622561.html

Erişim Tarihi 11.10.2020

www.timesonline.co.uk/article/0,,3-2289232,00.html

Erişim Tarihi 11.10.2020

### **Diğer Kaynaklar**

Akdağ, Polatkan, **Siber Suçlar ve Türkiye'nin Ulusal Politikası**, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara 2009. 222s.

Ankara Barosu Bilişim Programı Sertifika Programı Notları, 2007.

Aslanyürek, Malik, **İnternet Güvenliği ve Çevrimiçi Gizlilik Alanlarında Yaşanan Sorunlar: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları Üzerine Bir Araştırma**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara 2015, 219s.

Baezner, Marie ve Robin, Patrice, **Hotspot Analysis: Stuxnet**, Center for Security Studies (CSS), ETH Zurich, October 2017, 14s.

Coll, Steve ve Glasser Susan B., Terrorists Turn to the Web as Base of Operations, **The Washington Post**, 7 Ağustos 2005.

Devlet Planlama Teşkilatı, **Küreselleşme ve Özel İhtisas Raporu**, DPT yayını, Ankara 2000, 123s.

Ertürk, Volkan, **A Framework Based on Continuous Security Monitoring**, Orta Doğu Teknik Üniversitesi Bilişim Sistemleri Bölümü, Yüksek Lisans Tezi, Ankara 2008, 179s.

Hui, Lee Chih, **Information Technology Infrastructure Library (ITIL): An Approach To Optimize Best Practices In It Service Delivery**, Universty of Malaysia, 2012, 35s.

Koyuncu, Sefa, “Siber Terör”, **Türkiye Gazetesi**, 10 Haziran 2006.

Musharbash, Von Yassin, Terrorism in the Internet: The Cyber-Cemetery of the Mujahedeen, **Spiegel International**, 28 Ekim 2005.

Özkışlalı, Gizem, **Küreselleşme, İnternet ve Terörizmin Değişen Yüzü;Siber Terörizm**, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara 2008, 131s.

Parlak, Ahmet, **İnternet ve Türkiye’de İnternetin Gelişimi**, Fırat Üniversitesi Mühendislik Fakültesi, Bitirme Ödevi, Elazığ 2005, 87s.

Savaşlar, Zekai, **Küreselleşme ve Sosyal Boyutu**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul 2007, 189s.

T.C.Resmi Gazete, 12 Nisan 1991, Sayı:20843, 9s.

Timothy L. Thomas, “Al Qaeda and the Internet: The Danger of Cyberplanning”, **Parameters (Report)**, Cilt:23, Sayı:1, Bahar 2003, s.112-123.

Topal, Hikmet, **Siber Terör**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul 2004, 119s.

Turak, Yiğit, Redhack Özelinde Siber Olaylar ve Siber Suçlar, **Yayınlanmamış yayın**, 19s.

## **MEHMET SEĖMENOĐLU**

1985 yılında Adana’da doğdu. Lisans öğrenimini 2011’de Anadolu Üniversitesi İktisat Fakültesi’nde tamamladı. 2013’de Ege Üniversitesi Sosyal Bilimler Enstitüsü İşletme (Yönetim Bilimi ve Organizasyon) programında yüksek lisans öğrenimini tamamladı. Doktora öğrenimine Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi Sosyal Bilimler Enstitüsü İngilizce İşletme Doktora programında devam etmektedir.

**Orcid No.:** 0000-0003-1786-4473









**IKSAD**  
Publishing House



**ISBN: 978-625-7636-76-6**